Copia de seguridad y restauración del plano de control de vSphere IaaS

Actualización 3

VMware vSphere 8.0

VMware vCenter 8.0

VMware ESXi 8.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Copias de seguridad y restauración del plano de control de IaaS de vSphere

Copias de seguridad y restauración del plano de control de IaaS de vSphere proporciona información sobre cómo realizar una copia de seguridad y restaurar el plano de control del Supervisor, así como las cargas de trabajo que se ejecutan en los clústeres de Tanzu Kubernetes Grid y en pods de vSphere.

Audiencia prevista

Esta información está destinada a administradores de vSphere e ingenieros de desarrollo y operaciones que deseen realizar copias de seguridad y restaurar cargas de trabajo que se ejecutan en vSphere IaaS Control Plane, así como el estado del plano de control del Supervisor. Se requieren conocimientos en las siguientes áreas:

- vSphere IaaS Control Plane
- vSphere
- Kubernetes
- Velero
- Almacenamiento de instancias

Consideraciones para realizar copias de seguridad y restaurar vSphere IaaS Control Plane

1

Conozca cuál es el proceso de copia de seguridad y restauración de vSphere IaaS Control Plane, y familiarícese con las consideraciones generales para implementar una estrategia de copia de seguridad y restauración para vSphere IaaS Control Plane.

Situación	Tools	Comentarios
Copia de seguridad y restauración del plano de control del Supervisor	Copia de seguridad y restauración basada en archivos de vCenter Server desde la interfaz de usuario de administración de cargas de trabajo	Configure una copia de seguridad del estado de los Supervisores en vCenter Server como parte de las copias de seguridad basadas en archivos programadas en vCenter Server. Posteriormente, podrá restaurar el estado de los Supervisores en vCenter Server a través de la interfaz de administración de cargas de trabajo en vSphere Client. **Nota** La restauración del estado de los Supervisores en vCenter Server y la restauración del estado de vCenter Server son dos flujos de trabajo diferentes. La restauración de vCenter Server no conduce a la restauración de los Supervisores. Consulte Capítulo 2 Copia de seguridad y restauración del plano de control del Supervisor.
Copia de seguridad y restauración de pods de vSphere	complemento de Velero para vSphere	Instalar y configurar el complemento en el Supervisor. Consulte Capítulo 3 Instalar y configurar el complemento de Velero para vSphere en Supervisor. Consulte Capítulo 6 Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere.

Situación	Tools	Comentarios
Copia de seguridad de cargas de trabajo sin estado y con estado en un clúster de Tanzu Kubernetes Grid y restauración a un clúster aprovisionado por Tanzu Kubernetes Grid.	complemento de Velero para vSphere	Realice una copia de seguridad y restaure los metadatos de Kubernetes y los volúmenes persistentes. Puede usar la generación de snapshots de Velero (no Restic) para volúmenes persistentes. Consulte Capítulo 3 Instalar y configurar el complemento de Velero para vSphere en Supervisor. Consulte Realizar una copia de seguridad y restaurar cargas de trabajo de clústeres de TKG 2 mediante el complemento de Velero para vSphere.
Copia de seguridad de cargas de trabajo sin estado y con estado en un clúster de Tanzu Kubernetes Grid y restauración a un clúster de Kubernetes conforme no aprovisionado por Tanzu Kubernetes Grid.	Restic y Velero independientes	Utilice Velero independiente para la portabilidad. Debe incluir Restic para las aplicaciones con estado. Consulte Instalar y configurar Velero y Restic independientes en clústeres de TKG 2 en Supervisor. Consulte Realizar una copia de seguridad y restaurar cargas de trabajo en las cargas de trabajo de los clústeres de TKG 2 en el supervisor mediante Restic y Velero independientes.
Configuración de vCenter Server	vCenter Server	Si se pierde vCenter Server, utilice vCenter Server para realizar una copia de seguridad y restaurar los objetos de vCenter Server. Consulte Restaurar vCenter Server y crear una copia de seguridad de ella con base en archivos.
NSX	NSX Manager	El equilibrador de carga y los servicios de entrada dependen de la copia de seguridad de NSX. NSX-T Data Center proporciona una copia de seguridad y recuperación en el producto que admite la copia de seguridad y la restauración de los nodos y los objetos de NSX Manager. Para obtener más información, consulte Copia de seguridad y restauración de NSX Manager en la documentación de NSX-T.

Copia de seguridad y restauración del plano de control del Supervisor

2

Puede incluir la opción para registrar el estado de los Supervisores en vCenter Server como parte de las copias de seguridad basadas en archivos de vCenter Server. Más adelante, puede restaurar el plano de control del Supervisor a partir de los archivos de copia de seguridad creados.

Lea los siguientes temas a continuación:

- Realizar una copia de seguridad del estado del Supervisor
- Restaurar el plano de control del Supervisor

Realizar una copia de seguridad del estado del Supervisor

Aprenda a realizar una copia de seguridad del estado de los Supervisores en su entorno. Puede incluir la copia de seguridad de los Supervisores disponibles en vCenter Server como parte de las copias de seguridad basadas en archivos de vCenter Server.

Los archivos de copia de seguridad del plano de control del Supervisor capturan el estado de los siguientes componentes:

- El estado de etcd.
- Imágenes de contenedor que se utilizan en pods de infraestructura para garantizar que las máquinas virtuales del plano de control se puedan restaurar después de actualizar vCenter Server.
- La clave y el certificado de CA de Kubernetes para garantizar que todos los certificados de Kubernetes se puedan volver a generar después de una restauración desde la misma entidad de certificación. Esto garantiza que los pods de vSphere y Spherelet no tengan que volver a configurarse después de la restauración para confiar en una nueva entidad de certificación de Kubernetes.
- Todos los espacios de nombres de vSphere y el estado de todos los recursos de Kubernetes que están asociados con cargas de trabajo, como implementaciones, pods, máquinas virtuales, recursos de TKG, notificaciones de volumen persistente, etc.

Para obtener más información sobre la copia de seguridad y la restauración basadas en archivos de vCenter Server, consulte Restaurar vCenter Server y crear una copia de seguridad de ella con base en archivos.

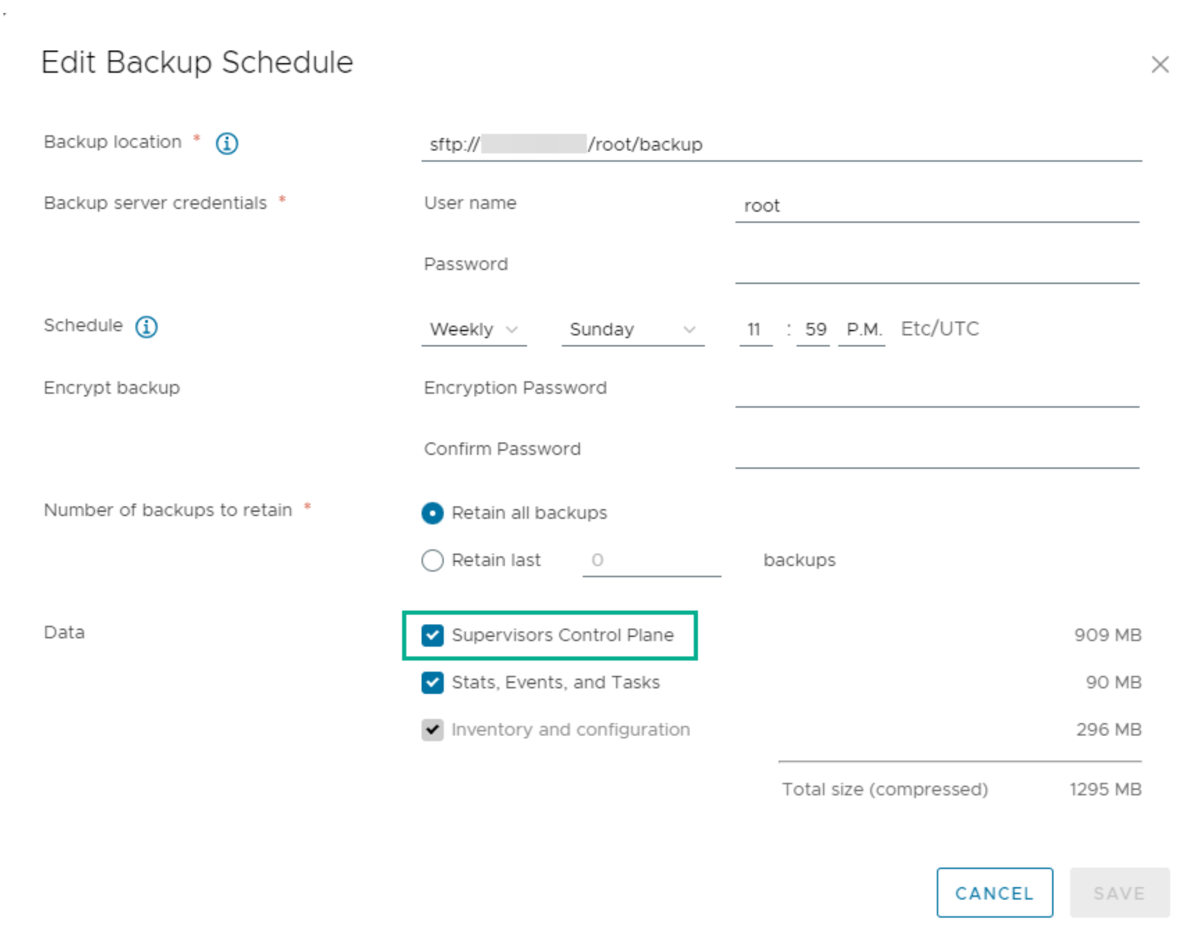
Requisitos previos

- Debe tener un servidor FTP, FTPS, HTTP, HTTPS, SFTP, NFS o SMB en funcionamiento con suficiente espacio de disco para poder almacenar la copia de seguridad.

Procedimiento

1. En un navegador web, vaya a la interfaz de administración de vCenter Server: `https://appliance-IP-address-or-FQDN:5480`.
2. Inicie sesión como raíz.
3. En la interfaz de administración de vCenter Server, haga clic en **Copia de seguridad**.
4. Haga clic en **Editar** si ya existe una programación de copia de seguridad.

   Si no existe una programación de copia de seguridad, consulte Programar una copia de seguridad basada en archivos para obtener información sobre cómo crear una.
5. En el panel Editar programación de copia de seguridad, seleccione **Plano de control de supervisores**.



Resultados

Se realiza una copia de seguridad del estado de todos los Supervisores de vCenter Server como parte de las copias de seguridad de vCenter Server.

Restaurar el plano de control del Supervisor

Puede restaurar el panel de control del Supervisores en vCenter Server a partir de los archivos de copia de seguridad del propio sistema vCenter Server.

Nota La restauración del plano de control de los Supervisores en vCenter Server y la restauración del estado de vCenter Server son dos flujos de trabajo diferentes. La restauración de vCenter Server no conduce a la restauración del plano de control del Supervisor.

Requisitos previos

- Configure el registro del estado del Supervisor desde las copias de seguridad basadas en archivos de la interfaz de administración de vCenter Server.

Procedimiento

1 En vSphere Client, desplácese hasta **Administración de cargas de trabajo**.

2 Seleccione **Supervisores** y **Restaurar**.

3 Introduzca los detalles de la copia de seguridad.

Opción	Descripción
vCenter	Seleccione el sistema vCenter Server que administra el Supervisor.
Selección de copia de seguridad	■ Seleccione **Carpeta del servidor de copia de seguridad** para cargar los archivos almacenados en la carpeta raíz del servidor de archivos de copia de seguridad configurado con este sistema vCenter Server. ■ Seleccione **Ubicación de copia de seguridad única** para cargar un archivo de copia de seguridad concreto y, a continuación, introduzca la dirección URL de ese archivo de copia de seguridad. ■ Seleccione **Usar la ubicación y el nombre de usuario de la copia de seguridad de la programación de copia de seguridad de vCenter** para rellenar la ubicación de la carpeta raíz y el nombre de usuario de la ubicación de la copia de seguridad que están configurados con vCenter Server.
Ubicación	Introduzca la ubicación de la carpeta raíz de copia de seguridad.
Nombre de usuario	Introduzca el nombre de usuario para acceder a las copias de seguridad
contraseña	Escriba la contraseña para ese nombre de usuario.

4 Haga clic en **Siguiente**.

5 Seleccione un archivo de copia de seguridad desde el que restaurar y haga clic en **Siguiente** para iniciar la descarga del archivo de copia de seguridad.

6 Seleccione el Supervisor que desea restaurar y haga clic en **Siguiente**.

7 Revise la configuración y haga clic en **Finalizar**.

Resultados

El Supervisor vuelve al estado de configuración y todas las máquinas virtuales del plano de control eliminadas se vuelven a implementar con los datos del archivo de copia de seguridad. Para supervisar el proceso, haga clic en **ver** en la columna **Estado de configuración**.

Instalar y configurar el complemento de Velero para vSphere en Supervisor

3

Aprenda a instalar y configurar el complemento de Velero para vSphere para realizar copias de seguridad y restauración de cargas de trabajo que se ejecutan en clústeres de TKG y pods de vSphere.

Descripción general

El complemento de Velero para vSphere proporciona una solución para hacer copias de seguridad y restauración de cargas de trabajo de vSphere IaaS Control Plane. Una vez que haya instalado y configurado el complemento de Velero para vSphere en Supervisor, puede realizar copias de seguridad y restaurar las cargas de trabajo del clúster de TKG y pods de vSphere. Para cargas de trabajo persistentes, el complemento de Velero para vSphere le permite tomar instantáneas de los volúmenes persistentes.

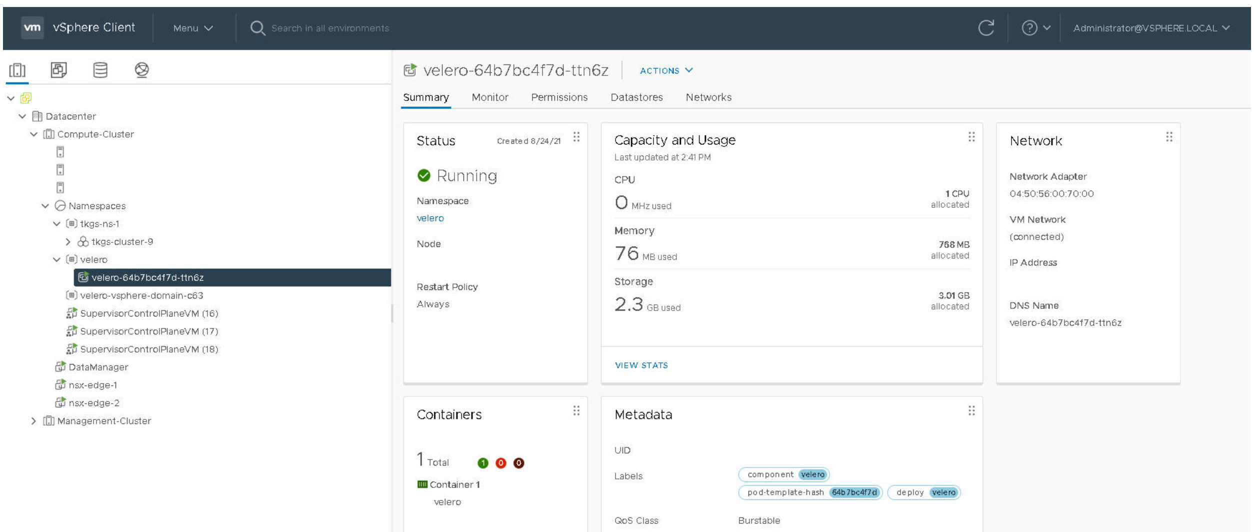
Requisitos previos:

- Supervisor está activado.
- Se crea y se configura una instancia de espacio de nombres de vSphere.
- Debe ser miembro de la función de administrador de vSphere o tener los siguientes privilegios de vSphere:
  - **SupervisorServices.Manage**
  - **Namespaces.Manage**
  - **Namespaces.Configure**

  Nota Consulte Crear un grupo y una función dedicados en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.
- Cree una máquina virtual Linux donde pueda ejecutar la CLI de Velero. O bien utilice un host de salto de Linux existente en el que acceda a Supervisor.
- Los números de versión de Velero se presentan como `X.Y.Z`. Consulte la Matriz de compatibilidad de Velero para ver las versiones específicas que deben utilizarse y sustitúyalas según corresponda al ejecutar los comandos.

La captura de pantalla muestra el estado final de una instalación de complemento de Velero para vSphere.

- Las redes NSX se utilizan para admitir la implementación de pods de vSphere.
- Hay una máquina virtual de Data Manager implementada.
- El operador Velero está activado y en ejecución en el espacio de nombres `velero-vsphere-domain-cXX`.
- Hay un espacio de nombres llamado `velero` configurado.
- El complemento de Velero para vSphere se ejecuta como un pod de vSphere en el espacio de nombres `velero`.



Paso 0 (opcional): Crear una red dedicada para el tráfico de copia de seguridad y restauración

Aunque no es necesario, se recomienda que, para los entornos de producción, separe el tráfico de copia de seguridad y restauración del tráfico de red de administración de vSphere IaaS Control Plane. Existen dos aspectos que se deben considerar sobre esto:

- Etiquete los hosts ESXi para admitir la copia de archivo de red (Network File Copy, NFC)
- Configure la red de copia de seguridad y restauración mediante NSX.

Para configurar hosts ESXi de modo que admitan un transporte de dispositivo de bloques de red (Network Block Device, NBD) dedicado, agregue una NIC de VMkernel en cada host ESXi de los clústeres de vSphere donde se ejecute el Supervisor y establezca `vSphereBackupNFC` en esa NIC. Cuando se aplica la etiqueta `vSphereBackupNFC` al tipo de NIC para un adaptador de VMkernel, el tráfico de copia de seguridad y restauración pasa por la NIC virtual seleccionada.

Para realizar esta configuración, utilice Virtual Disk Development Kit. Consulte la documentación del NBD.

Nota Si la `vSphereBackupNFC` no está habilitada en la NIC de VMkernel, el tráfico de copia de seguridad y restauración no se enviará a la red de copia de seguridad y restauración, aunque configure una. Si no se habilita `vSphereBackupNFC`, el tráfico viajará por la red de administración de vSphere.

Una vez habilitada la etiqueta de `vSphereBackupNFC`, configure la red de copia de seguridad y restauración mediante NSX; para ello, actualice la instancia de vSphere Distributed Switch (VDS) existente para el clúster de la siguiente manera:

- En vSphere Client, seleccione **Menú > Redes**.
- Seleccione el VDS existente para el clúster.
- Haga clic con el botón secundario en el VDS y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.
- Cree un nuevo grupo de puertos distribuidos denominado **BackupRestoreNetwork**.
- Agregue un adaptador de VMkernel al grupo de puertos distribuidos **BackupRestoreNetwork**.
- Asocie todos los hosts ESXi del clúster de vCenter en el que la Administración de cargas de trabajo está habilitada al grupo de puertos distribuidos **BackupRestoreNetwork**.
- Habilite la etiqueta `vSphereBackupNFC`.

Paso 1: Crear un almacén de objetos compatible con S3

Para realizar copias de seguridad y restauraciones de volúmenes persistentes, debe proporcionar un almacén de objetos compatible con S3. Velero admite varios proveedores de almacenes objetos.

Para instalar el complemento de Velero para vSphere, debe proporcionar la siguiente información sobre el almacén de objetos compatible con S3:

Elemento de datos	Valor de ejemplo
s3Url	http://my-s3-store.example.com
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Cree un nombre de archivo de secretos `s3-credentials` con la siguiente información. Debe hacer referencia a este archivo cuando instale el complemento de Velero para vSphere.

```
[default]
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

MinIO es un almacén de objetos compatible con S3 que es fácil de instalar y utilizar. vSphere IaaS Control Plane se incluye con un servicio de supervisor de MinIO que puede habilitar. Para obtener más información, consulte la publicación *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

Como alternativa, puede instalar manualmente un servidor MinIO en una máquina virtual Linux. Para obtener instrucciones, consulte Instalar y configurar Velero y Restic independientes en clústeres de TKG.

Paso 2: Instalar y configurar Data Manager

Advertencia Data Manager solo se ha probado funcionalmente; no está pensado para funcionar a escala y no promete ninguna expectativa de rendimiento. No está pensado para realizar copias de seguridad de las aplicaciones decisivas en producción.

Para facilitar la copia de seguridad y la restauración mediante el complemento de Velero para vSphere, implemente una o varias máquinas virtuales de Data Manager para mover los datos de copia de seguridad de volúmenes persistentes dentro y fuera del almacenamiento de objetos compatible con S3. Data Manager mueve los datos de instantáneas de volumen desde el volumen de vSphere hasta el almacenamiento compatible con S3 remoto y durable en la copia de seguridad, y desde el almacenamiento compatible con S3 remoto hasta un volumen de vSphere durante la restauración.

En un entorno de vSphere IaaS Control Plane, instale Data Manager como máquina virtual.

Nota No encienda la máquina virtual de Data Manager hasta que haya habilitado operador para vSphere de Velero.

1 Con vSphere Client, haga clic con el botón secundario en el centro de datos donde está activado el Supervisor y seleccione **Implementar plantilla de OVF**.

2 Descargue en el equipo local el archivo OVA de Data Manager desde la siguiente URL: https://vmwaresaas.jfrog.io/artifactory/Velero-YAML/Velero/DataManager/1.2.0/datamgr-ob-20797900-photon-3-release-1.2.ova.

3 Seleccione **Archivo local** y cargue el archivo OVA de Data Manager en vCenter Server.

4 Asigne un nombre a la máquina virtual, como `DataManager`, por ejemplo.

5 Seleccione el recurso informático que es el clúster de vSphere en el que está configurado el Supervisor.

6 Revise los detalles de la implementación de la máquina virtual y haga clic en **Siguiente**.

7 Acepte los acuerdos de licencia y haga clic en **Siguiente**.

8 Seleccione el almacenamiento y haga clic en **Siguiente**.

9 Seleccione la red de destino para la máquina virtual de Data Manager.

   - Seleccione la **BackupRestoreNetwork** si configuró una red de copia de seguridad y restauración dedicada.
   - Seleccione la **red de administración** si no configuró una red de copia de seguridad y restauración dedicada.

10 Confirme las selecciones y haga clic en **Finalizar** para completar el proceso.

11 Utilice el panel Tareas recientes para supervisar el progreso de la implementación.

   Nota Si recibe un error que indica "el descriptor de OVF no está disponible", utilice el navegador Chrome.

12 Una vez implementada la máquina virtual de Data Manager, configure los parámetros de entrada de la máquina virtual.

13 Haga clic con el botón secundario en la máquina virtual y seleccione **Editar configuración**.

14 En la pestaña Hardware virtual, para Unidad de CD/DVD, cambie de **Dispositivo host** a **Dispositivo cliente**.

   Nota Si no lo hace, no podrá guardar las opciones de configuración avanzada requeridas.

15 En la pestaña **Editar configuración > Parámetros avanzados**, seleccione **Avanzado > Editar parámetros de configuración**.

16 Configure los parámetros de entrada para cada una de las siguientes opciones:

Parámetro	Valor
`guestinfo.cnsdp.vcUser`	Introduzca el nombre de usuario de vCenter Server con privilegios suficientes para implementar máquinas virtuales. Si no especifica un usuario con permisos de administrador de vSphere, consulte la documentación de Permisos de vSphere para obtener instrucciones. O bien, cree un usuario dedicado para la administración de cargas de trabajo. Consulte Crear un grupo y una función dedicados en *Uso del servicio TKG con el plano de control de IaaS de vSphere*.
`guestinfo.cnsdp.vcAddress`	Introduzca la dirección IP o el FQDN de vCenter Server.
`guestinfo.cnsdp.vcPasswd`	Introduzca la contraseña de usuario de vCenter Server.
`guestinfo.cnsdp.vcPort`	El valor predeterminado es **443**. No cambie este valor.
`guestinfo.cnsdp.wcpControlPlaneIP`	Introduzca la dirección IP flotante del Supervisor. Para obtener este valor, desplácese hasta el Supervisor en Administración de cargas de trabajo y seleccione **Configurar > Red > Red de administración > IP flotante**
`guestinfo.cnsdp.updateKubectl`	El valor predeterminado es **false**. No cambie este valor.

Parámetro	Valor
`guestinfo.cnsdp.veleroNamespace`	Deje el valor predeterminado: `velero`. Más adelante en el proceso, debe crear un espacio de nombres de vSphere en el Supervisor con el nombre `velero`. Estos dos nombres deben coincidir.
`guestinfo.cnsdp.datamgrImage`	Si no está configurado (sin establecer), el sistema extrae de forma predeterminada la imagen de contenedor de Docker Hub en `vsphereveleroplugin/data-manager-for-plugin:1.1.0`

17 Haga clic en **Aceptar** para guardar la configuración y en **Aceptar** nuevamente para guardar la configuración de la máquina virtual.

Nota Si no cambió la unidad de CD/DVD de **Dispositivo host** a **Dispositivo cliente**, no podrá guardar la configuración. Si este es el caso, cancele la operación, cambie la unidad y repita los ajustes de configuración avanzada.

18 No encienda la máquina virtual de Data Manager hasta después de habilitar operador para vSphere de Velero (siguiente sección).

Paso 3: Instalar el servicio de operador para vSphere de Velero en Supervisor

vSphere IaaS Control Plane proporciona el operador para vSphere de Velero como servicio de supervisor. El servicio operador para vSphere de Velero funciona con el complemento de Velero para vSphere para admitir la copia de seguridad y la restauración de cargas de trabajo de Kubernetes, incluida la creación de instantáneas de volúmenes persistentes. Para obtener más información sobre los servicios de supervisor, consulte Administrar servicios de supervisor en *Servicios y cargas de trabajo del plano de control de IaaS de vSphere*.

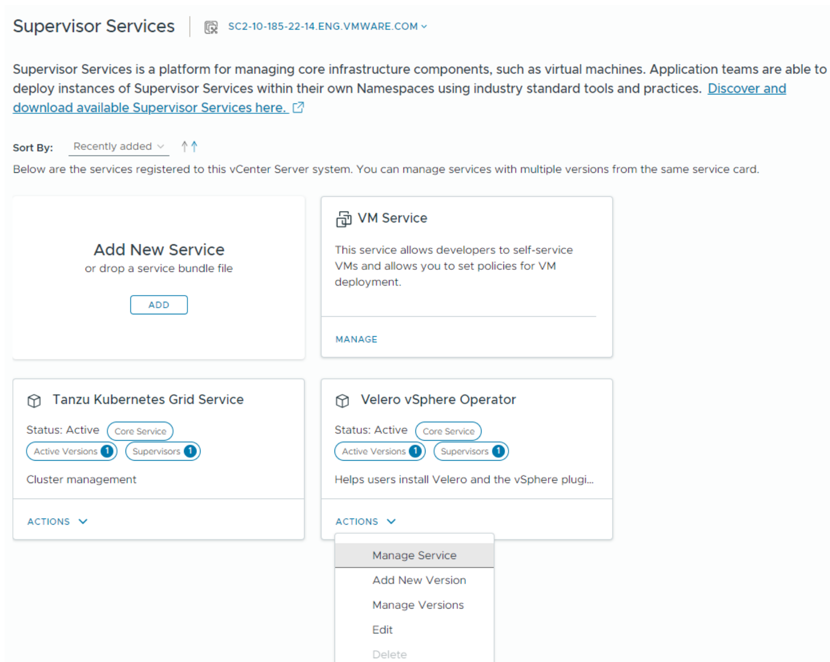
El operador para vSphere de Velero es un servicio de supervisor principal, lo que significa que el operador de servicio viene prerregistrado con vCenter Server. Complete los pasos para instalar el operador para vSphere de Velero como un servicio en Supervisor.

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione la pestaña **Servicios**.

3 Seleccione la instancia de vCenter Server de destino en el menú desplegable de la parte superior.

4 En la tarjeta del operador para vSphere de Velero, seleccione **Acciones > Gestionar servicio**.



5 Seleccione el Supervisor de destino donde desee instalar el servicio y haga clic en **Siguiente**.

6 Haga clic en **Finalizar** para completar la instalación del servicio.

Compruebe el servicio operador para vSphere de Velero en el Supervisor e inicie la máquina virtual de Data Manager.

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**.

3 Compruebe que puede ver que el operador para vSphere de Velero está instalado y que su estado es **Configurado**.

4 En la pestaña **Espacios de nombres**, compruebe que ve un nuevo espacio de nombres espacio de nombres de vSphere denominado `svc-velero-vsphere-domain-xxx`, donde `xxx` es un token alfanumérico único. Este es el espacio de nombres que crea el sistema para el operador para vSphere de Velero.

   Nota No es necesario configurar este espacio de nombres y no debe editarlo.

5 En **Hosts y clústeres**, busque la máquina virtual de Data Manager y encienda la máquina virtual.

Paso 4: Crear un espacio de nombres de vSphere para el complemento de Velero para vSphere

Con vSphere Client, cree manualmente un espacio de nombres de vSphere en el Supervisor. Este espacio de nombres de vSphere es obligatorio para el complemento de Velero para vSphere.

- Asigne el nombre **`velero`** al espacio de nombres de vSphere.
- Seleccione el espacio de nombres **velero** y configúrelo.
- Especifique el almacenamiento para el espacio de nombres **velero**.
- Otorgue a un usuario con los privilegios adecuados el permiso Editar en el espacio de nombres **velero**.

Paso 5: Crear el mapa de configuración del complemento de Velero para vSphere

Cree un mapa de configuración para el complemento de Velero para vSphere denominado `velero-vsphere-plugin-config.yaml`.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: velero-vsphere-plugin-config
data:
  cluster_flavor: SUPERVISOR
```

Aplique el mapa de configuración al Supervisor.

```
kubectl apply -n <velero-namespace> -f velero-vsphere-plugin-config.yaml
```

Si no instala el mapa de configuración, recibirá el siguiente error cuando intente instalar el complemento de Velero para vSphere.

```
Error received while retrieving cluster flavor from config, err: configmaps "velero-vsphere-
plugin-config" not found
Falling back to retrieving cluster flavor from vSphere CSI Driver Deployment
```

Paso 6: Instalar el complemento de Velero para vSphere

Ahora ya está listo para instalar el complemento de Velero para vSphere. Para ello, descargue y ejecute la CLI **velero-vsphere**.

Nota Este procedimiento requiere una máquina virtual Linux. Descargue el archivo binario **velero-vsphere** en el host de salto de Linux en el que ejecuta las CLI `kubectl-vsphere` y `kubectl`.

1 Descargue la CLI del complemento de Velero para vSphere.

Compruebe la matriz de compatibilidad y descargue la versión de destino desde aquí: https://github.com/vmware-tanzu/velero-plugin-for-vsphere/releases.

Nota En los siguientes comandos, reemplace `X.Y.Z` por las versiones de la CLI y el complemento de Velero que haya descargado.

---

2 Copie de forma segura la CLI en el host de salto de Linux. Por ejemplo:

```
pscp -P 22 C:\temp\velero-vsphere-X.Y.Z-linux-amd64.tar.gz ubuntu@10.117.29.131:/home/
ubuntu/tanzu
```

3 Extraiga la CLI `velero-vsphere` y haga que permita escritura.

```
tar -xf velero-vsphere-X.Y.Z-linux-amd64.tar.gz
chmod +x velero-vsphere
```

4 Agregue la CLI a la ruta de acceso.

```
export PATH="$(pwd)/velero-vsphere-X.Y.Z-linux-amd64:$PATH"
```

5 Cree el archivo `s3-credentials` con el siguiente contenido.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

6 Obtenga la región, la URL y el nombre del depósito para el almacén de objetos compatible con S3.

7 Inicie sesión en Supervisor mediante complemento de vSphere para kubectl.

8 Cambie el contexto al Supervisor.

```
kubectl config use-context SUPERVISOR-CLUSTER-IP-ADDRESS
```

9 Ejecute el siguiente comando de la CLI `velero-vsphere` para instalar el complemento de Velero para vSphere en el espacio de nombres **velero** que creó.

Exporte los valores de **`$BUCKET`** y **`$REGION`** de AWS. Si se desvió de cualquiera de las instrucciones anteriores, ajuste también esos valores, como el nombre o la ubicación del archivo de secretos, el nombre del espacio de nombres `velero` creado manualmente, etc.

```
export BUCKET=example-velero-sv && export REGION=us-east-1

./velero-vsphere install \
       --namespace velero \
       --version vX.X.X \
       --provider aws \
       --plugins harbor-repo.vmware.com/velero/velero-plugin-for-aws:vX.Y.Z,harbor-
repo.vmware.com/velero/velero-plugin-for-vsphere:vX.Y.Z \
```

```
        --bucket $BUCKET \
        --secret-file ~/.aws/credentials \
        --snapshot-location-config region=$REGION \
        --backup-location-config region=$REGION
```

Nota Por ejemplo, la versión de la CLI de Velero es la 1.8.1 si se utiliza complemento de Velero para vSphere v1.4.0.

10 Compruebe que la instalación del complemento de Velero para vSphere se haya realizado correctamente.

Cuando la instalación se realiza correctamente, debería ver el siguiente mensaje:

```
Send the request to the operator about installing Velero in namespace velero
```

Ejecute el siguiente comando para realizar una verificación adicional. Debería ver "Completado" y la versión.

```
kubectl -n velero get veleroservice default -o json | jq '.status'
```

Resultado esperado:

```
{
  "enabled": true,
  "installphase": "Completed",
  "version": "v1.8.1"
}
```

Nota El comando anterior asume que tiene instalada la utilidad `jq`, que formatea la salida JSON enviada al terminal. Si no tiene `jq` instalada, instálela o elimine esa parte del comando (todo después de `json`).

11 Solucione problemas según sea necesario.

Si la instalación no se realiza correctamente, elimine la instalación e inténtelo de nuevo. Para eliminar la instalación, complete los pasos de la siguiente sección en el orden indicado.

Anexo: Desinstalar el complemento de Velero para vSphere

Siga estos pasos para desinstalar el complemento de Velero para vSphere.

1 Ejecute la CLI `velero-vsphere` para desinstalar el complemento de Velero para vSphere.

```
./velero-vsphere uninstall -n velero
```

2 Compruebe que se haya eliminado el pod de vSphere denominado `velero`.

```
kubectl get pods -n velero
```

Si ve que el pod está "Finalizando", espere a que se elimine antes de continuar.

3 Con vSphere Client, elimine el espacio de nombres de vSphere denominado `velero` que creó manualmente.

Nota No continúe con el siguiente paso hasta que se complete la eliminación del espacio de nombres. Puede utilizar kubectl para comprobar que se eliminó el espacio de nombres `velero` (pero no utilice kubectl para eliminar el espacio de nombres `velero`).

Anexo: Instalar el complemento de Velero para vSphere en un entorno aislado

Si tiene pensado instalar el complemento de Velero para vSphere en un entorno aislado, debe hacerlo con imágenes personalizadas. Debe asegurarse de que las imágenes coincidentes de `backup-driver` y `data-manager-for-plugin` de las imágenes personalizadas estén disponibles en el registro esperado y que se pueda acceder a ellas desde el clúster de Kubernetes. En un entorno aislado, se esperan imágenes personalizadas del registro privado, ya que no es posible acceder a las imágenes publicadas en Docker Hub.

Para instalar el complemento, realice los siguientes pasos:

1 Descargue las imágenes publicadas de `velero-plugin-for-vsphere`, `backup-driver` y `data-manager-for-plugin`.

2 Cambie el nombre de las imágenes; es decir, etiquételas con los `<Registry endpoint and path>` y `<Version tag>` coincidentes y cárguelas en los repositorios personalizados.

3 Instale el complemento utilizando la imagen `velero-plugin-for-vsphere` que personalizó.

   Cuando instale el complemento de Velero para vSphere en un clúster básico, se implementan dos componentes adicionales: una implementación de `backup-driver` y un DaemonSet de `data-manager-for-plugin` en segundo plano. En los clústeres de Tanzu Kubernetes y el Supervisor, solo se procede con una implementación de `backup-driver`.

   Cuando se proporciona la imagen de contenedor de `velero-plugin-for-vsphere`, las imágenes de `backup-driver` y `data-manager-for-plugin` coincidentes se analizan mediante un mecanismo de análisis de imágenes.

   Las imágenes de contenedor se formalizan con el siguiente patrón:

```
<Registry endpoint and path>/<Container name>:<Version tag>
```

   Cuando se proporciona la imagen de contenedor de `velero-plugin-for-vsphere`, se analizan las imágenes correspondientes de `backup-driver` y `data-manager-for-plugin` con las coincidentes de `<Registry endpoint and path>` y `<Version tag>`.

   Por ejemplo, tenga en cuenta la siguiente imagen de contenedor de `velero-plugin-for-vsphere`:

```
abc.io:8989/x/y/.../z/velero-plugin-for-vsphere:vX.Y.Z
```

Se espera que se extraigan las siguientes imágenes coincidentes de `backup-driver` y `data-manager-for-plugin`:

```
abc.io:8989/x/y/.../z/backup-driver:vX.Y.Z
abc.io:8989/x/y/.../z/data-manager-for-plugin:vX.Y.Z
```

4 Solucione los problemas de la instalación.

Si se produce algún problema o error al analizar las imágenes coincidentes de `backup-driver` y `data-manager-for-plugin`, la instalación recurre a las imágenes correspondientes de los repositorios oficiales de `velerovsphereplugin` en Docker Hub. Los siguientes problemas activan el mecanismo de reserva:

a En la entrada del usuario, se utiliza un nombre de contenedor inesperado en la imagen de `velero-plugin-for-vsphere` personalizada.

Por ejemplo, se utiliza `x/y/velero-velero-plugin-for-vsphere:vX.Y.Z`.

b El nombre de la implementación de Velero se personaliza con cualquier otra opción que no sea `velero`. Por ejemplo, se activa un problema si el nombre de la implementación de Velero se actualiza a `velero-server` en el archivo `manifests` de Velero antes de implementar Velero.

El mecanismo de análisis de imágenes que hay actualmente en `velero-plugin-for-vsphere` solo puede reconocer la implementación de Velero con el nombre fijo, `velero`.

Copia de seguridad y restauración de cargas de trabajo y clústeres de servicio TKG

4

Consulte esta sección para realizar copias de seguridad y restaurar las cargas de trabajo y los clústeres de servicio TKG.

Lea los siguientes temas a continuación:

- Consideraciones para realizar copias de seguridad y restaurar cargas de trabajo y clústeres de Servicio TKG
- Copia de seguridad y restauración de cargas de trabajo de clústeres de TKG mediante complemento de Velero para vSphere
- Realizar una copia de seguridad y restaurar cargas de trabajo de clústeres de TKG en Supervisor mediante Restic y Velero independientes
- Copia de seguridad y restauración mediante Velero con instantánea de CSI

Consideraciones para realizar copias de seguridad y restaurar cargas de trabajo y clústeres de Servicio TKG

En este tema se ofrecen las consideraciones que hay que tener en cuenta para realizar copias de seguridad y restaurar las cargas de trabajo que se ejecutan en clústeres de Servicio TKG.

Hacer una copia de seguridad y restaurar clústeres de Servicio TKG

Para realizar una copia de seguridad y restaurar clústeres de TKG, realice una copia de seguridad de la base de datos de Supervisor. Si lo hace, podrá restaurar objetos de espacios de nombres de vSphere y máquinas virtuales de nodo de clústeres de TKG.

Habilite la copia de seguridad y restauración de Supervisor mediante la función de copia de seguridad de vCenter Server disponible a través de la interfaz de administración de vCenter Server. Para obtener más información, consulte la publicación de restauración de copia de seguridad de vSphere IaaS Control Plane.

Nota Puede utilizar la copia de seguridad de Supervisor solo para restaurar las máquinas virtuales del nodo de clúster de TKG. No se puede utilizar la copia de seguridad de Supervisor para restaurar las cargas de trabajo implementadas en clústeres de TKG. Debe realizar una copia de seguridad de las cargas de trabajo por separado y, a continuación, restaurarlas después de restaurar el clúster.

Copia de seguridad y restauración de cargas de trabajo que se ejecutan en clústeres de Servicio TKG

En esta tabla se resumen las opciones para hacer copias de seguridad y restaurar cargas de trabajo sin estado y con estado que se ejecutan en clústeres de TKG.

Nota La copia de seguridad y la restauración de un clúster de Kubernetes mediante Velero independiente le ofrece portabilidad. Esto significa que si desea poder restaurar las cargas de trabajo del clúster en un clúster de Kubernetes no aprovisionado por Servicio TKG, debe utilizar Velero independiente.

Situación	Herramienta	Comentarios
Haga una copia de seguridad de las cargas de trabajo sin estado y con estado en un clúster de TKG en Supervisor y restaure en un clúster de TKG en Supervisor.	Complemento de Velero para vSphere Consulte Copia de seguridad y restauración de cargas de trabajo de clústeres de TKG mediante complemento de Velero para vSphere.	Se puede realizar una copia de seguridad y restaurar tanto los metadatos de Kubernetes como los volúmenes persistentes. La creación de instantáneas de Velero se utiliza para volúmenes persistentes con aplicaciones con estado. Requiere que el complemento de Velero para vSphere también esté instalado y configurado en supervisor.
Haga una copia de seguridad de las cargas de trabajo sin estado y con estado en un clúster de TKG en Supervisor y restaure en un clúster de Kubernetes compatible.	Restic y Velero independientes Consulte Realizar una copia de seguridad y restaurar cargas de trabajo de clústeres de TKG en Supervisor mediante Restic y Velero independientes. .	Se puede realizar una copia de seguridad y restaurar tanto los metadatos de Kubernetes como los volúmenes persistentes. Restic se utiliza para volúmenes persistentes con aplicaciones con estado. Utilice este enfoque si necesita portabilidad.
Haga una copia de seguridad de las cargas de trabajo sin estado y con estado en un clúster de TKG en Supervisor y restaure en un clúster de Kubernetes compatible.	Instancia de Velero independiente con instantáneas de CSI Consulte Copia de seguridad y restauración mediante Velero con instantánea de CSI.	Requiere vSphere 8.0 U2+ y TKr v1.26+ para vSphere 8.0.

Copia de seguridad y restauración de cargas de trabajo de clústeres de TKG mediante complemento de Velero para vSphere

En esta sección se proporcionan temas para hacer copias de seguridad y restaurar cargas de trabajo de clústeres de TKG que se ejecutan en Supervisor mediante el complemento de Velero para vSphere.

Instalar y configurar el complemento de Velero para vSphere en un clúster de TKG

Es posible utilizar el complemento de Velero para vSphere para realizar una copia de seguridad y una restauración de las cargas de trabajo que se ejecutan en un clúster de TKGS mediante la instalación del complemento de Velero para vSphere en ese clúster.

Descripción general

complemento de Velero para vSphere proporciona una solución para realizar una copia de seguridad y una restauración de las cargas de trabajo de clústeres de Servicio TKG. Para cargas de trabajo persistentes, el complemento de Velero para vSphere le permite tomar instantáneas de los volúmenes persistentes.

Nota Si necesita portabilidad para las cargas de trabajo del clúster de Servicio TKG de las que desea realizar una copia de seguridad y restauración, no utilice el complemento de Velero para vSphere. Para la portabilidad entre clústeres de Kubernetes, utilice Velero independiente con Restic.

Requisito previo: instale el complemento de Velero para vSphere en el Supervisor

Para la instalación del complemento de Velero para vSphere en un clúster de TKGS, se requiere que el Supervisor tenga instalado el complemento de Velero para vSphere. Además, Supervisor debe estar configurado con redes NSX. Consulte Capítulo 3 Instalar y configurar el complemento de Velero para vSphere en Supervisor.

Requisito de almacenamiento

Para realizar una copia de seguridad del clúster de Servicio TKG, necesita un back-end de almacenamiento como se describe en este documento. Si va a realizar una copia de seguridad de varios clústeres, no debe utilizar el mismo back-end de almacenamiento para diferentes copias de seguridad de clústeres. Si comparte el back-end de almacenamiento, se sincronizarán los objetos de copia de seguridad. Debe utilizar un back-end de almacenamiento diferente para evitar el escape de datos.

Paso 1: Instalar la CLI de Velero en una Workstation de Linux

La CLI de Velero es la herramienta estándar para interactuar con Velero. La CLI de Velero proporciona más funcionalidad que la CLI del complemento de Velero para vSphere (`velero-vsphere`) y es necesaria para realizar copias de seguridad y restauración de las cargas de trabajo del clúster de Tanzu Kubernetes.

Instale la CLI de Velero en una estación de trabajo Linux. Idealmente, este es el mismo host de salto en el que se ejecutan las CLI asociadas para el entorno de vSphere IaaS Control Plane, incluidos `kubectl`, `kubectl-vsphere` y `velero-vsphere`.

Los números de versión de Velero se presentan como `X.Y.Z`. Consulte la Matriz de compatibilidad de Velero para ver las versiones específicas que deben utilizarse y sustitúyalas según corresponda al ejecutar los comandos.

Complete los siguientes pasos para instalar la CLI de Velero.

1 Ejecute los siguientes comandos:

```
$ wget https://github.com/vmware-tanzu/velero/releases/download/vX.Y.Z/velero-vX.Y.Z-linux-amd64.tar.gz
$ gzip -d velero-vX.Y.Z-linux-amd64.tar.gz && tar -xvf velero-vX.Y.Z-linux-amd64.tar
$ export PATH="$(pwd)/velero-vX.Y.Z-linux-amd64:$PATH"

$ which velero
/root/velero-vX.Y.Z-linux-amd64/velero
```

2 Compruebe la instalación de la CLI de Velero.

```
velero version

Client:
    Version: vX.Y.Z
```

Paso 2: Obtener los detalles del depósito compatible con S3

Para mayor comodidad, los pasos asumen que está utilizando el mismo almacén de objetos compatible con S3 que configuró cuando instaló el complemento de Velero para vSphere en el Supervisor. En producción, es posible que desee crear un almacén de objetos independiente.

Para instalar el complemento de Velero para vSphere, deberá proporcionar la siguiente información sobre el almacén de objetos compatible con S3.

Elemento de datos	Valor de ejemplo
s3Url	`http://my-s3-store.example.com`
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Cree un nombre de archivo de secretos `s3-credentials` con la siguiente información. Debe hacer referencia a este archivo cuando instale el complemento de Velero para vSphere.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

Paso 3 Opción A: Instalar complemento de Velero para vSphere en el clúster de TKG con una etiqueta (nuevo método)

Si utiliza vSphere 8 Update 3 o una versión posterior, puede instalar complemento de Velero para vSphere automáticamente en un clúster de TKG agregando una etiqueta.

1 Compruebe que se pueda acceder a la ubicación de almacenamiento de la copia de seguridad.

2 Compruebe que esté activada la función servicio de supervisor de Velero vSphere Operator Core.

```
kubectl get ns | grep velero
svc-velero-domain-c9                          Active   18d
```

3 Compruebe que se haya creado un espacio de nombres de Kubernetes con el nombre `velero` en Supervisor.

```
kubectl get ns | grep velero
svc-velero-domain-c9                          Active   18d
velero                                        Active   1s
```

4 Compruebe que servicio de supervisor de complemento de Velero para vSphere esté habilitado en Supervisor.

```
velero version
Client:
        Version: v1.11.1
        Git commit: bdbe7eb242b0f64d5b04a7fea86d1edbb3a3587c
Server:
        Version: v1.11.1
```

```
kubectl get veleroservice -A
NAMESPACE   NAME      AGE
velero      default   53m
```

```
velero backup-location get
NAME      PROVIDER   BUCKET/PREFIX   PHASE       LAST VALIDATED                  ACCESS
MODE   DEFAULT
default   aws        velero          Available   2023-11-20 14:10:57 -0800 PST
ReadWrite     true
```

5 Agregue la etiqueta velero al clúster a fin de habilitar Velero para el clúster de TKG de destino.

```
kubectl label cluster CLUSTER-NAME --namespace CLUSTER-NS velero.vsphere.vmware.com/
enabled=true
```

Nota Esto se realiza desde espacio de nombres de vSphere cuando se aprovisiona el clúster.

6 Compruebe que Velero esté instalado y listo para el clúster.

```
kubectl get ns
NAME                                 STATUS   AGE
...
velero                               Active   2m    <--
velero-vsphere-plugin-backupdriver   Active   2d23h
```

```
kubectl get all -n velero
NAME                                 READY   STATUS    RESTARTS   AGE
pod/backup-driver-5945d6bcd4-gtw9d   1/1     Running   0          17h
pod/velero-6b9b49449-pq6b4           1/1     Running   0          18h
NAME                            READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/backup-driver   1/1     1            1           17h
deployment.apps/velero          1/1     1            1           18h
NAME                                       DESIRED   CURRENT   READY   AGE
replicaset.apps/backup-driver-5945d6bcd4   1         1         1       17h
replicaset.apps/velero-6b9b49449           1         1         1       18h
```

```
velero version
Client:
        Version: v1.11.1
        Git commit: bdbe7eb242b0f64d5b04a7fea86d1edbb3a3587c
Server:
        Version: v1.11.1
```

Paso 3 Opción B: Instalar complemento de Velero para vSphere en el clúster de TKG manualmente (método heredado)

Deberá utilizar la CLI de Velero para instalar el complemento de Velero para vSphere en el clúster de TKG de destino del que desea realizar una copia de seguridad y restauración.

El contexto de la CLI de Velero seguirá automáticamente el contexto de `kubectl`. Antes de ejecutar los comandos de la CLI de Velero para instalar Velero y el complemento de Velero para vSphere en el clúster de destino, asegúrese de establecer el contexto de `kubectl` en el clúster de destino.

1 Utilice el complemento de vSphere para kubectl para autenticarse en el Supervisor.

2 Establezca el contexto de `kubectl` en el clúster de TKG de destino.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

3 En el clúster de TKG, cree un mapa de configuración para el complemento de Velero denominado `velero-vsphere-plugin-config.yaml`.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: velero-vsphere-plugin-config
data:
  cluster_flavor: GUEST
```

Aplique el mapa de configuración en el clúster de TKG.

```
kubectl apply -n <velero-namespace> -f velero-vsphere-plugin-config.yaml
```

Si no instala el mapa de configuración, recibirá el siguiente error cuando intente instalar el complemento de Velero para vSphere.

```
Error received while retrieving cluster flavor from config, err: configmaps "velero-vsphere-plugin-config" not found
Falling back to retrieving cluster flavor from vSphere CSI Driver Deployment
```

4 Ejecute el siguiente comando de la CLI de Velero para instalar Velero en el clúster de destino.

Reemplace los valores de marcador de posición de los campos **`BUCKET-NAME`**, **`REGION`** (dos instancias) y **`s3Url`** con los valores adecuados. Si se desvió de cualquiera de las instrucciones anteriores, ajuste también esos valores, como el nombre o la ubicación del archivo de secretos, el nombre del espacio de nombres `velero` creado manualmente, etc.

```
./velero install --provider aws \
--bucket BUCKET-NAME \
--secret-file ./s3-credentials \
--features=EnableVSphereItemActionPlugin \
--plugins velero/velero-plugin-for-aws:vX.Y.Z \
--snapshot-location-config region=REGION \
--backup-location-config region=REGION,s3ForcePathStyle="true",s3Url=http://my-s3-store.example.com
```

5 Instale el complemento de Velero para vSphere en el clúster de destino. El Velero instalado se comunicará con el servidor de API de Kubernetes para instalar el complemento.

```
velero plugin add vsphereveleroplugin/velero-plugin-for-vsphere:vX.Y.Z
```

Anexo: Desinstalar el complemento de Velero para vSphere del clúster de TKG

Siga estos pasos para desinstalar el complemento de Velero para vSphere.

1 Establezca el contexto de `kubectl` en el clúster de destino de Tanzu Kubernetes.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

2 Para desinstalar el complemento, ejecute el siguiente comando para eliminar el InitContainer de velero-plugin-for-vsphere de la implementación de Velero.

```
velero plugin remove vsphereveleroplugin/velero-plugin-for-vsphere:vX.Y.Z
```

3 Para completar el proceso, elimine la implementación del controlador de copia de seguridad y los CRD relacionados.

```
kubectl -n velero delete deployment.apps/backup-driver
```

```
kubectl delete crds \
backuprepositories.backupdriver.cnsdp.vmware.com \
backuprepositoryclaims.backupdriver.cnsdp.vmware.com \
clonefromsnapshots.backupdriver.cnsdp.vmware.com \
deletesnapshots.backupdriver.cnsdp.vmware.com \
snapshots.backupdriver.cnsdp.vmware.com
```

```
kubectl delete crds uploads.datamover.cnsdp.vmware.com downloads.datamover.cnsdp.vmware.com
```

Realizar una copia de seguridad y restaurar cargas de trabajo de clúster de TKG mediante complemento de Velero para vSphere

Puede realizar copias de seguridad y restaurar cargas de trabajo que se ejecutan en clústeres de TKG en Supervisor mediante el complemento de Velero para vSphere.

Requisitos previos

Para realizar una copia de seguridad y restaurar cargas de trabajo de los clústeres de TKG mediante el complemento de Velero para vSphere, primero debe instalar el complemento de Velero para vSphere en el clúster de destino. Consulte Instalar y configurar el complemento de Velero para vSphere en un clúster de TKG.

Copia de seguridad de una carga de trabajo

A continuación se muestra un comando de ejemplo para crear una copia de seguridad de Velero.

```
velero backup create <backup name> --include-namespaces=my-namespace
```

La copia de seguridad de Velero se marcará como `Completed` después de que se hayan tomado todas las instantáneas locales y se hayan cargado los metadatos de Kubernetes, excepto las instantáneas de volumen, en el almacén de objetos. En este punto, las tareas de movimiento de datos asincrónicas, es decir, la carga de instantáneas de volumen, aún se están realizando en segundo plano y pueden tardar algún tiempo en completarse. Podemos comprobar el estado de las instantáneas de volumen mediante la supervisión de los recursos personalizados (CR) de instantánea.

Snapshots

Las instantáneas se utilizan para realizar copias de seguridad de volúmenes persistentes. Para cada instantánea de volumen, se crea un CR de instantánea en el mismo espacio de nombres que la notificación de volumen persistente (PVC) de que se crea una instantánea.

Puede obtener todas las instantáneas en el espacio de nombres de PVC ejecutando el siguiente comando.

```
kubectl get -n <pvc namespace> snapshot
```

La definición de recursos personalizados (CRD) de instantánea tiene varias fases para el campo `.status.phase`, que incluyen lo siguiente:

Fase de instantánea	Descripción
Novedad	Aún no procesada
Snapshotted	Se tomó una instantánea local
SnapshotFailed	Se produjo un error en la instantánea local
Uploading	Se está cargando la instantánea
Uploaded	Se cargó la instantánea
UploadFailed	No se pudo cargar la instantánea
Canceling	Se está cancelando la carga de la instantánea
Canceled	Se canceló la carga de la instantánea
CleanupAfterUploadFailed	Se produjo un error en la limpieza de la instantánea local después de la carga de la instantánea

Restaurar una carga de trabajo

A continuación se muestra un comando de ejemplo de restauración de Velero.

```
velero restore create --from-backup <velero-backup-name>
```

La restauración de Velero se marcará como `Completed` cuando las instantáneas de volumen y otros metadatos de Kubernetes se hayan restaurado correctamente en el clúster actual. En este punto, también se completan todas las tareas del complemento de vSphere relacionadas con esta restauración. No hay tareas de movimiento de datos asincrónicas en segundo plano como en el caso de la copia de seguridad de Velero.

CloneFromSnapshots

Para restaurar desde cada instantánea de volumen, se creará un recurso personalizado (CR) `CloneFromSnapshot` en el mismo espacio de nombres que la PVC que se creó originalmente. Podemos obtener todos los CloneFromSnapshots de PVC ejecutando el siguiente comando.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

CloneFromSnapshot CRD tiene algunas fases clave para el campo `.status.phase`:

Fase de instantánea	Descripción
Novedad	No se completó la clonación de la instantánea
InProgress	La instantánea del volumen de vSphere se está descargando desde el repositorio remoto

Fase de instantánea	Descripción
Completed	Se completó la clonación de la instantánea
Con errores	Error en la clonación de la instantánea

Realizar una copia de seguridad y restaurar cargas de trabajo de clústeres de TKG en Supervisor mediante Restic y Velero independientes

En esta sección se proporcionan temas para hacer copias de seguridad y restaurar cargas de trabajo de clústeres de TKG que se ejecutan en Supervisor mediante Velero con Restic independientes.

Instalar y configurar Velero y Restic independientes en clústeres de TKG

Para realizar copias de seguridad y restauración de cargas de trabajo en clústeres de TKG en Supervisor, cree un almacén de datos e instale Velero con Restic en el clúster de Kubernetes.

Descripción general

Los clústeres de TKG se ejecutan en nodos de la máquina virtual. Para realizar una copia de seguridad y restaurar cargas de trabajo de clústeres de TKG, instale Velero y Restic en el clúster.

Requisitos previos

Asegúrese de que el entorno cumpla con los siguientes requisitos previos para instalar Velero y Restic a fin de realizar copias de seguridad y restauración de cargas de trabajo que se ejecutan en clústeres de Tanzu Kubernetes.

- Una máquina virtual Linux con suficiente almacenamiento para almacenar varias copias de seguridad de cargas de trabajo. Debe instalar MinIO en esta máquina virtual.
- Una máquina virtual Linux en la que están instaladas Herramientas de la CLI de Kubernetes para vSphere, lo que incluye complemento de vSphere para kubectl y kubectl. Debe instalar la CLI de Velero en esta máquina virtual cliente. Si no tiene una máquina virtual de este tipo, puede instalar la CLI de Velero de forma local, pero debe ajustar los pasos de instalación según corresponda.
- El entorno de Kubernetes tiene acceso a Internet y la máquina virtual cliente puede acceder a él.

Instalar y configurar el almacén de objetos minIO

Velero requiere un almacén de objetos compatible con S3 como el destino de las copias de seguridad de la cargas de trabajo de Kubernetes. Velero admite varios proveedores de almacenes de objetos de este tipo. Por simplicidad, estas instrucciones utilizan MinIO, un servicio de almacenamiento compatible con S3 que se ejecuta localmente en la máquina virtual del almacén de objetos.

1 Instale MinIO.

```
wget https://dl.min.io/server/minio/release/linux-amd64/minio
```

2 Otorgue permisos de ejecución a MinIO.

```
chmod +x minio
```

3 Cree un directorio en el sistema de archivos para MinIO.

```
mkdir /DATA-MINIO
```

4 Inicie el servidor MinIO.

```
./minio server /DATA-MINIO
```

5 Una vez iniciado el servidor MinIO, se le proporcionarán detalles importantes de la instancia del almacén de datos, incluidos la URL del endpoint, AccessKey y SecretKey. Registre la URL de endpoint, AccessKey y SecretKey en la tabla.

Metadatos del almacén de datos	Valor
URL de endpoint	
AccessKey	
SecretKey	

6 Abra un navegador a la URL del endpoint del servidor MinIO y desplácese hasta el almacén de datos de MinIO.

7 Inicie sesión en el servidor MinIO y proporcione AccessKey y SecretKey.

8 Para habilitar MinIO como servicio, descargue el script `minio.service` para configurar MinIO para inicio automático.

```
curl -O https://raw.githubusercontent.com/minio/minio-service/master/linux-systemd/
minio.service
```

9 Edite el script `minio.service` y agregue el siguiente valor para `ExecStart`.

```
ExecStart=/usr/local/bin/minio server /DATA-MINIO path
```

10 Guarde el script revisado.

11 Configure el servicio MinIO mediante la ejecución de los siguientes comandos.

```
cp minio.service /etc/systemd/system
cp minio /usr/local/bin/
systemctl daemon-reload
systemctl start minio
systemctl status minio
systemctl enable minio
```

12 Cree un depósito MinIO para realizar una copia de seguridad y restauración; para ello, inicie el explorador MinIO e inicie sesión en el almacén de objetos.

13 Haga clic en el icono Crear depósito.

14 Introduzca el nombre del depósito, por ejemplo: `my-cluster-backups`.

15 Compruebe que se haya creado el depósito.

16 De forma predeterminada, un nuevo depósito MinIO es de solo lectura. Para una copia de seguridad y restauración independientes de Velero, el depósito MinIO debe ser de lectura y escritura. Para establecer el depósito en lectura y escritura, selecciónelo y haga clic en el vínculo de puntos suspensivos (puntos).

17 Seleccione **Editar directiva**.

18 Cambie la directiva a **Lectura y escritura**.

19 Haga clic en **Agregar**.

20 Para cerrar el cuadro de diálogo, haga clic en la X.

Instalar la CLI de Velero

Instale la CLI de Velero en el cliente de máquina virtual o en la máquina local.

La versión que se utilizó para esta documentación es *Velero 1.9.7 para Tanzu Kubernetes Grid 2.2.0*.

1 Descargue Velero desde la página de descarga del producto Tanzu Kubernetes Grid en el portal de VMware Customer Connect.

Nota Debe utilizar el archivo binario de Velero firmado por VMware para poder recibir soporte de VMware.

2 Abra una línea de comandos y cambie el directorio a la descarga de la CLI de Velero.

3 Descomprima el archivo de descarga. Por ejemplo:

```
gunzip velero-linux-vX.X.X_vmware.1.gz
```

4 Compruebe el archivo binario de Velero.

```
ls -l
```

5 Otorgue permisos de ejecución a la CLI de Velero.

```
chmod +x velero-linux-vX.X.X_vmware.1
```

6 Haga que la CLI de Velero esté disponible globalmente, para ello, muévala a la ruta del sistema:

```
cp velero-linux-vX.X.X_vmware.1 /usr/local/bin/velero
```

7 Compruebe la instalación.

```
velero version
```

Instalar Velero y Restic en el clúster de Tanzu Kubernetes

El contexto de la CLI de Velero seguirá automáticamente el contexto de kubectl. Antes de ejecutar los comandos de la CLI de Velero para instalar Velero y Restic en el clúster de destino, establezca el contexto de kubectl.

1 Recupere el nombre del depósito MinIO. Por ejemplo, `my-cluster-backups`.

2 Obtenga AccessKey y SecretKey para el depósito MinIO.

3 Establezca el contexto del clúster de Kubernetes de destino para que la CLI de Velero sepa en qué clúster trabajar.

```
kubectl config use-context tkgs-cluster-name
```

4 Cree un archivo de secretos denominado `credentials-minio`. Actualice el archivo con las credenciales de acceso al servidor MinIO que recopiló. Por ejemplo:

```
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

Nota Si recibe el mensaje de error "Error al obtener un almacén de copias de seguridad" con la descripción "NoCredentialProviders: no hay proveedores válidos en la cadena", anteponga la línea `[default]` al principio del archivo de credenciales. Por ejemplo:

```
[default]
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

5 Guarde el archivo y compruebe que esté en su lugar.

```
ls
```

6 Ejecute el siguiente comando para instalar Velero y Restic en el clúster de Kubernetes de destino. Reemplace ambas URL por la URL de la instancia de MinIO.

```
velero install \
--provider aws \
--plugins velero/velero-plugin-for-aws:v1.0.0 \
--bucket tkgs-velero \
--secret-file ./credentials-minio \
--use-volume-snapshots=false \
--use-restic \
--backup-location-config \
region=minio,s3ForcePathStyle="true",s3Url=http://10.199.17.63:9000,publicUrl=http://
10.199.17.63:9000
```

7 Compruebe la instalación de Velero y Restic.

```
kubectl logs deployment/velero -n velero
```

8 Compruebe el espacio de nombres `velero`.

```
kubectl get ns
```

9 Compruebe los pods `velero` y `restic`.

```
kubectl get all -n velero
```

Solucionar problemas de DaemonSet de Restic (si es necesario)

Para ejecutar el DaemonSet de Restic de tres pods en un clúster de Kubernetes, es posible que deba actualizar la especificación de DaemonSet de Restic y modificar el hostPath. Para obtener más información sobre este problema, consulte Integración de Restic en la documentación de Velero.

1 Compruebe el DaemonSet de Restic de tres pods.

```
kubectl get pod -n velero
```

Si los pods tienen el estado CrashLoopBackOff, edítelos de la siguiente manera.

2 Ejecute el comando `edit`.

```
kubectl edit daemonset restic -n velero
```

3 Cambie hostPath de `/var/lib/kubelet/pods` a `/var/vcap/data/kubelet/pods`.

```
- hostPath:
    path: /var/vcap/data/kubelet/pods
```

4 Guarde el archivo.

5 Compruebe el DaemonSet de Restic de tres pods.

```
kubectl get pod -n velero
```

```
NAME                       READY   STATUS    RESTARTS   AGE
restic-5jln8               1/1     Running   0          73s
restic-bpvtq               1/1     Running   0          73s
restic-vg8j7               1/1     Running   0          73s
velero-72c84322d9-le7bd    1/1     Running   0          10m
```

Ajustar los límites de memoria de Velero (si es necesario)

Si la copia de seguridad de Velero devuelve `status=InProgress` durante muchas horas, aumente la configuración de memoria para límites y solicitudes.

1 Ejecute el siguiente comando.

```
kubectl edit deployment/velero -n velero
```

2 Cambie la configuración de memoria para límites y solicitudes desde el valor predeterminado de `256Mi` y `128Mi` a `512Mi` y `256Mi`.

```
ports:
- containerPort: 8085
  name: metrics
  protocol: TCP
resources:
  limits:
    cpu: "1"
    memory: 512Mi
  requests:
    cpu: 500m
    memory: 256Mi
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
```

Copia de seguridad y restauración de cargas de trabajo de clúster mediante Restic y Velero independientes

Puede realizar operaciones de copia de seguridad y restauración de las cargas de trabajo que se ejecutan en los clústeres de TKG mediante Velero y Restic independientes. Este método es una alternativa al uso de un complemento complemento de Velero para vSphere. La razón principal para usar Velero independiente es la necesidad de portabilidad. Se requiere Restic para las cargas de trabajo con estado.

Requisitos previos

Para realizar copias de seguridad y restaurar cargas de trabajo en clústeres de TKG mediante Restic y Velero independientes, debe instalar la versión independiente de estos en el clúster de destino. Si la restauración se va a realizar en un clúster de destino independiente, Velero y Restic también deben estar instalados en el clúster de destino. Consulte Instalar y configurar Velero y Restic independientes en clústeres de TKG.

Realizar una copia de seguridad de una aplicación sin estado que se ejecuta en un clúster de TKG

La copia de seguridad de una aplicación sin estado que se ejecuta en un clúster de TKG requiere el uso de Velero.

En este ejemplo se muestra cómo realizar una copia de seguridad y restaurar una aplicación sin estado de ejemplo mediante la etiqueta `--include namespaces` en la que todos los componentes de la aplicación se encuentran en ese espacio de nombres.

```
velero backup create example-backup --include-namespaces example-backup
```

Debería ver el siguiente mensaje:

```
Backup request "example-backup" submitted successfully.
Run `velero backup describe example-backup` or `velero backup logs example-backup` for more
details.
```

Compruebe la copia de seguridad que se creó.

```
velero backup get
```

```
velero backup describe example-backup
```

Compruebe el depósito Velero en el almacén de objetos compatible con S3, como el servidor MinIO.

Velero escribe algunos metadatos en definiciones de recursos personalizados (Custom Resource Definitions, CRD) de Kubernetes.

```
kubectl get crd
```

Las CRD de Velero permiten ejecutar ciertos comandos, como los siguientes:

```
kubectl get backups.velero.io -n velero
```

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Restaurar una aplicación sin estado en ejecución en un clúster de TKG

La restauración de una aplicación sin estado que se ejecuta en un clúster de TKG requiere el uso de Velero.

Para probar la restauración de una aplicación de ejemplo, elimínela.

Elimine el espacio de nombres:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Restaure la aplicación:

```
velero restore create --from-backup example-backup
```

Debería ver el siguiente mensaje:

```
Restore request "example-backup-20200721145620" submitted successfully.
Run `velero restore describe example-backup-20200721145620` or `velero restore logs example-
backup-20200721145620` for more details.
```

Compruebe que la aplicación se restauró:

```
velero restore describe example-backup-20200721145620
```

Ejecute los siguientes comandos para comprobar:

```
velero restore get
```

```
kubectl get ns
```

```
kubectl get pod -n example
```

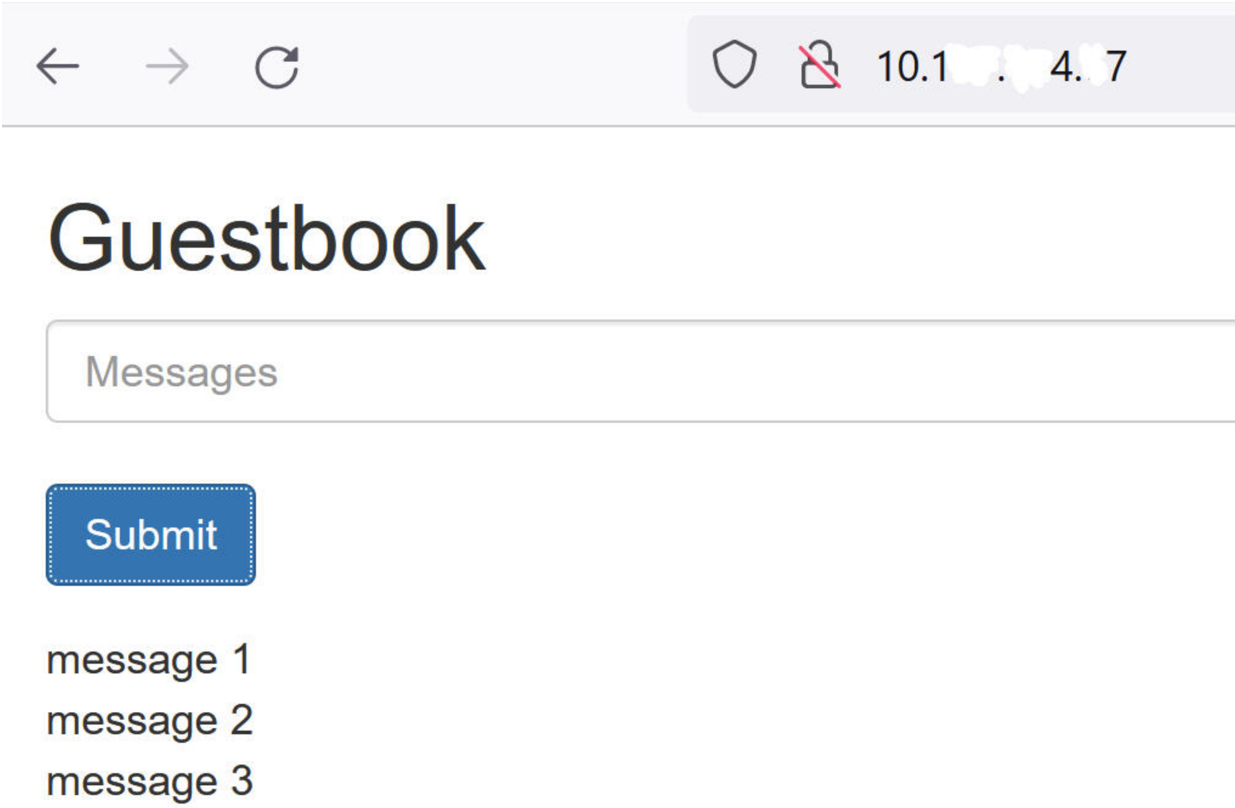
```
kubectl get svc -n example
```

Realizar una copia de seguridad de una aplicación con estado que se ejecuta en un clúster de TKG

Realizar una copia de seguridad de una aplicación con estado que se ejecuta en un clúster de TKG implica realizar una copia de seguridad de los metadatos de la aplicación y los datos de la aplicación almacenados en un volumen persistente. Para ello, necesita Velero y Restic.

En este ejemplo, utilizaremos la aplicación del libro de visitas. Si se supone que implementó la aplicación del libro de visitas en un clúster de TKG. Consulte #unique_17.

Para que podamos demostrar una copia de seguridad y una restauración con estado, envíe un mensaje a la aplicación del libro de visitas mediante la página web de front-end para que los mensajes persistan. Por ejemplo:



En este ejemplo se muestra cómo realizar una copia de seguridad y restaurar la aplicación del libro de visitas mediante la etiqueta `--include namespace`, así como las anotaciones del pod.

Nota En este ejemplo, se utilizan anotaciones. Sin embargo, ya no se necesitan anotaciones para Velero 1.5 y versiones posteriores. Para no utilizar anotaciones, puede usar la opción `--default-volumes-to-restic` al crear la copia de seguridad. Esto hará una copia de seguridad automática de todos los VA mediante Restic. Consulte https://velero.io/docs/v1.5/restic/ para obtener más información.

Para comenzar el procedimiento de copia de seguridad, obtenga los nombres de los pods:

```
kubectl get pod -n guestbook
```

Por ejemplo:

```
kubectl get pod -n guestbook

NAME                                            READY   STATUS    RESTARTS   AGE
guestbook-frontend-deployment-85595f5bf9-h8cff  1/1     Running          0          55m
guestbook-frontend-deployment-85595f5bf9-lw6tg  1/1     Running          0          55m
guestbook-frontend-deployment-85595f5bf9-wpqc8  1/1     Running          0          55m
redis-leader-deployment-64fb8775bf-kbs6s        1/1     Running          0          55m
redis-follower-deployment-84cd76b975-jrn8v      1/1     Running          0          55m
redis-follower-deployment-69df9b5688-zml4f      1/1     Running          0          55m
```

Los volúmenes persistentes se asocian a los pods de Redis. Debido a que estamos realizando una copia de seguridad de estos pods con estado con Restic, es necesario agregar anotaciones a los pods con estado con el nombre `volumeMount`.

Debe conocer `volumeMount` para anotar el pod con estado. Para obtener `mountName`, ejecute el siguiente comando.

```
kubectl describe pod redis-leader-deployment-64fb8775bf-kbs6s -n guestbook
```

En los resultados, verá `Containers.leader.Mounts: /data` de `redis-leader-data`. Este último token es el nombre `volumeMount` que se utilizará para la anotación del pod principal. Para el seguidor, será `redis-follower-data`. También puede obtener el nombre de `volumeMount` del YAML de origen.

Anote cada uno de los pods de Redis, por ejemplo:

```
kubectl -n guestbook annotate pod redis-leader-64fb8775bf-kbs6s backup.velero.io/backup-
volumes=redis-leader-data
```

Debería ver el siguiente mensaje:

```
pod/redis-leader-64fb8775bf-kbs6s annotated
```

Verifique las anotaciones:

```
kubectl -n guestbook describe pod redis-leader-64fb8775bf-kbs6s | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-leader-data
```

```
kubectl -n guestbook describe pod redis-follower-779b6d8f79-5dphr | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-follower-data
```

Realice la copia de seguridad de Velero:

```
velero backup create guestbook-backup --include-namespaces guestbook
```

Debería ver el siguiente mensaje:

```
Backup request "guestbook-backup" submitted successfully.
Run `velero backup describe guestbook-pv-backup` or `velero backup logs guestbook-pv-backup`
for more details.
```

Compruebe la copia de seguridad que se creó.

```
velero backup get

NAME                  STATUS      ERRORS   WARNINGS   CREATED
EXPIRES   STORAGE LOCATION   SELECTOR
guestbook-backup      Completed   0        0          2020-07-23 16:13:46 -0700 PDT
29d       default            <none>
```

Compruebe los detalles de la copia de seguridad.

```
velero backup describe guestbook-backup --details
```

Tenga en cuenta que Velero permite ejecutar otros comandos, como:

```
kubectl get backups.velero.io -n velero

NAME               AGE
guestbook-backup   4m58s
```

Y:

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Restaurar una aplicación con estado que se ejecuta en un clúster de TKG 2.0

La restauración de una aplicación con estado que se ejecuta en un clúster de TKG implica restaurar tanto los metadatos de la aplicación como los datos de la aplicación almacenados en un volumen persistente. Para ello, necesita Velero y Restic.

En este ejemplo, se supone que se realizó una copia de seguridad de la aplicación de libro de visitas con estado, como se describe en la sección anterior.

Para probar la restauración de la aplicación con estado, elimine su espacio de nombres:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Verifique la eliminación de la aplicación:

```
kubectl get ns
kubectl get pvc,pv --all-namespaces
```

Para restaurar una aplicación desde una copia de seguridad, utilice la siguiente sintaxis de comandos.

```
velero restore create --from-backup <velero-backup-name>
```

Por ejemplo:

```
velero restore create --from-backup guestbook-backup
```

Deben aparecer mensajes similares al siguiente:

```
Restore request "guestbook-backup-20200723161841" submitted successfully.
Run `velero restore describe guestbook-backup-20200723161841` or `velero restore logs
guestbook-backup-20200723161841` for more details.
```

Compruebe que se restauró la aplicación del libro de visitas con estado:

```
velero restore describe guestbook-backup-20200723161841

Name:         guestbook-backup-20200723161841
Namespace:    velero
Labels:       <none>
Annotations:  <none>

Phase:  Completed

Backup:  guestbook-backup

Namespaces:
  Included:  all namespaces found in the backup
  Excluded:  <none>

Resources:
  Included:        *
  Excluded:        nodes, events, events.events.k8s.io, backups.velero.io,
restores.velero.io, resticrepositories.velero.io
  Cluster-scoped:  auto

Namespace mappings:  <none>

Label selector:  <none>

Restore PVs:  auto

Restic Restores (specify --details for more information):
  Completed:  3
```

Ejecute el siguiente comando adicional para verificar la restauración:

```
velero restore get

NAME                                BACKUP              STATUS      ERRORS   WARNINGS
CREATED                        SELECTOR
guestbook-backup-20200723161841     guestbook-backup    Completed   0        0
2021-08-11 16:18:41 -0700 PDT   <none>
```

Compruebe que se restauró el espacio de nombres:

```
kubectl get ns

NAME               STATUS   AGE
default            Active   16d
guestbook          Active   76s
...
velero             Active   2d2h
```

Compruebe que la aplicación se restauró:

```
vkubectl get all -n guestbook

NAME                                READY   STATUS    RESTARTS   AGE
pod/frontend-6cb7f8bd65-h2pnb       1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-kwlpr       1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-snwl4       1/1     Running   0          6m27s
pod/redis-leader-64fb8775bf-kbs6s   1/1     Running   0          6m28s
pod/redis-follower-779b6d8f79-5dphr 1/1     Running   0          6m28s
pod/redis-follower-899c7e2z65-8apnk 1/1     Running   0          6m28s

NAME                                 TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE
service/guestbook-frontend           LoadBalancer   10.10.89.59      10.19.15.99
80:31513/TCP   65s
service/redis-follower               ClusterIP      10.111.163.189   <none>
6379/TCP       65s
service/redis-leader                 ClusterIP      10.111.70.189    <none>
6379/TCP       65s

NAME                                            READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/guestbook-frontend-deployment   3/3     3            3           65s
deployment.apps/redis-follower-deployment       1/2     2            1           65s
deployment.apps/redis-leader-deployment         1/1     1            1           65s

NAME                                                       DESIRED   CURRENT   READY   AGE
replicaset.apps/guestbook-frontend-deployment-56fc5b6b47   3         3         3       65s
replicaset.apps/redis-follower-deployment-6fc9cf5759       2         2         1       65s
replicaset.apps/redis-leader-deployment-7d89bbdbcf         1         1         1       65s
```

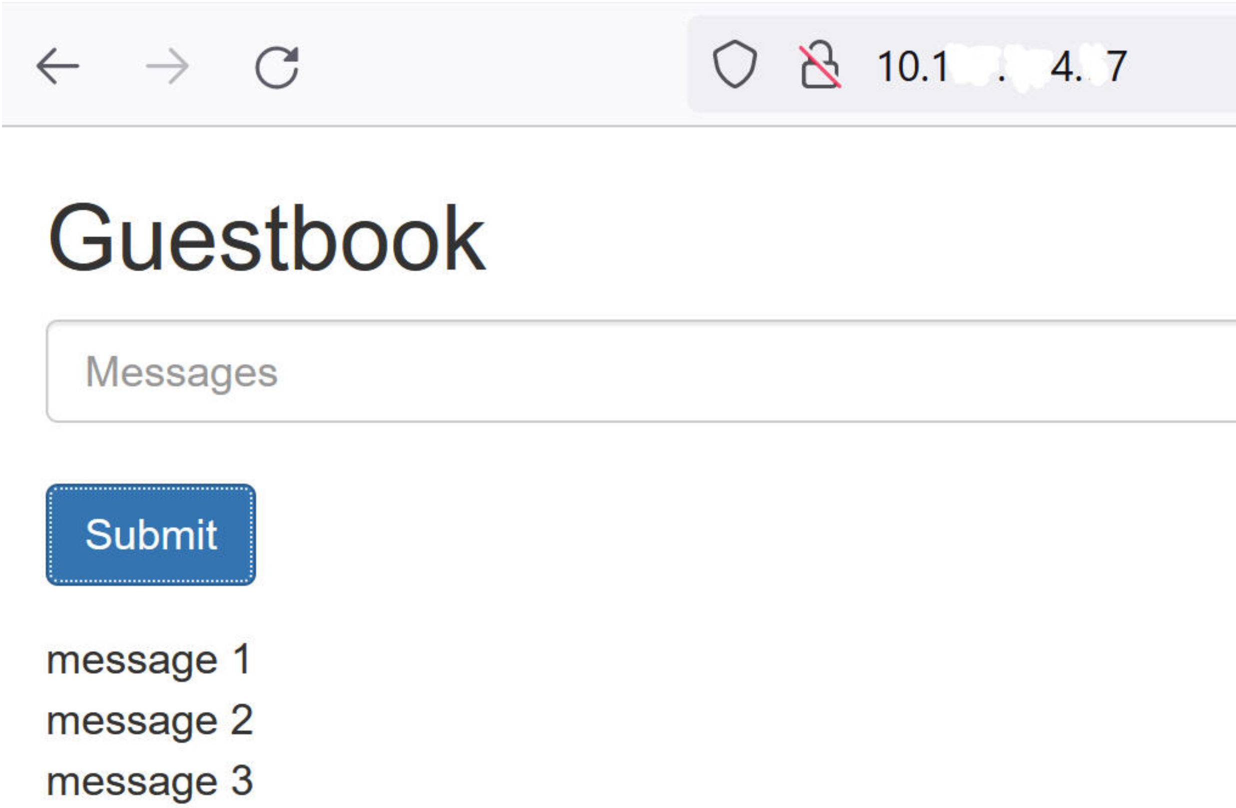
Compruebe que se restauren los volúmenes persistentes:

```
kubectl get pvc,pv -n guestbook

NAME                                       STATUS
VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/redis-leader-claim   Bound    pvc-a2f6e6d4-42db-4fb8-
a198-5379a2552509   2Gi        RWO            thin-disk      2m40s
persistentvolumeclaim/redis-follower-claim Bound    pvc-55591938-921f-452a-
b418-2cc680c0560b   2Gi        RWO            thin-disk      2m40s

NAME                                                        CAPACITY   ACCESS MODES   RECLAIM
POLICY   STATUS   CLAIM                             STORAGECLASS   REASON   AGE
persistentvolume/pvc-55591938-921f-452a-b418-2cc680c0560b   2Gi        RWO
Delete           Bound    guestbook/redis-follower-claim    thin-disk               2m40s
persistentvolume/pvc-a2f6e6d4-42db-4fb8-a198-5379a2552509   2Gi        RWO
Delete           Bound    guestbook/redis-leader-claim      thin-disk               2m40s
```

Por último, acceda al front-end del libro de visitas mediante la dirección IP externa del servicio de front-end del libro de visitas y compruebe que se restauren los mensajes que envió al principio del tutorial. Por ejemplo:



Copia de seguridad y restauración mediante Velero con instantánea de CSI

Puede utilizar Velero con instantánea de CSI para realizar una copia de seguridad y una restauración de los volúmenes persistentes creados por CSI para cargas de trabajo que se ejecutan en clústeres de TKG aprovisionados en Supervisor.

Requisitos

Cumpla con los siguientes requisitos:

- vSphere 8.0 U2 o versiones posteriores
- Tanzu Kubernetes 1.26.5 para vSphere 8.x o versiones posteriores
- Volúmenes persistentes creados con controladores de CSI compatibles con instantáneas de volumen

---

Atención El uso de Velero con instantánea de CSI solo está disponible para volúmenes persistentes creados con controladores de CSI que admiten instantáneas de volumen. Consulte Crear instantáneas en un clúster de TKG en *Uso del servicio TKG con el plano de control de IaaS de vSphere* para obtener más información.

Procedimiento

Puede utilizar Velero con una instantánea de interfaz de almacenamiento de contenedores (Container Storage Interface, CSI) para realizar copias de seguridad y restauración de cargas de trabajo que se ejecutan en clústeres de TKGS. El agente del nodo de Velero es un DaemonSet que aloja módulos para completar tareas concretas de copia de seguridad y restauración mediante el movimiento de datos de instantáneas de CSI. Para obtener más información, consulte Compatibilidad con instantáneas de interfaz de almacenamiento de contenedores en Velero.

1 Cree una ubicación de almacenamiento compatible con S3, como MinIO o un contenedor AWS S3.

   En el siguiente ejemplo, se utiliza un contenedor AWS S3.

   Para utilizar MinIO, consulte Instalar y configurar el almacén de objetos minIO.

2 Instale la CLI de Velero en el cliente de clúster en el que está ejecutando kubectl.

   Descárguela desde https://github.com/vmware-tanzu/velero/releases.

   Consulte las instrucciones de instalación en uno de los siguientes vínculos:

   - Paso 1: Instalar la CLI de Velero en una Workstation de Linux
   - Instalar la CLI de Velero
   - https://velero.io/docs/v1.12/basic-install/#install-the-cli

3 Conéctese al clúster de Servicio TKG en el que desea ejecutar la copia de seguridad de Velero.

   Consulte Conexión a un clúster de servicio TKG como usuario de vCenter Single Sign-On con Kubectl.

4 Instale Velero con el complemento de la CLI de Velero en el clúster.

   A partir de la versión 1.14 de Velero, el complemento CSI de Velero se combina con Velero. Por lo tanto, si va a instalar Velero v1.14 o una versión posterior, no es necesario instalar el complemento CSI de Velero por separado. Si lo hace, el pod de Velero no se inicia.

   Por ejemplo, el siguiente comando instala Velero con un back-end de almacenamiento de AWS S3 y el archivo de credenciales correspondiente. Dado que es Velero v1.14, no es necesario instalar el complemento CSI de Velero por separado.

```
velero install \
    --provider aws \
    --plugins velero/velero-plugin-for-aws:v1.14 \
    --bucket velero-cpe-backup-bucket \
    --secret-file ./cloud-credential \
    --use-volume-snapshots=true \
    --features=EnableCSI --use-node-agent
```

Para instalar una versión anterior de Velero, también debe instalar el complemento CSI de Velero. Por ejemplo:

```
velero install \
    --provider aws \
    --plugins velero/velero-plugin-for-aws:v1.9.0,velero/velero-plugin-for-csi:v0.7.0 \
    --bucket velero-cpe-backup-bucket \
    --secret-file ./cloud-credential \
    --use-volume-snapshots=true \
    --features=EnableCSI --use-node-agent
```

Copia de seguridad y restauración de máquinas virtuales de servicio de máquina virtual en vSphere IaaS Control Plane

5

Como administrador de vSphere, utiliza soluciones de partners de copia de seguridad basadas en VMware vSphere Storage APIs – Data Protection (VADP) para realizar automáticamente una copia de seguridad, una restauración completa y el registro de una máquina virtual de servicio de máquina virtual en un Supervisor. Si se produce un error en el registro automático debido a problemas con la infraestructura subyacente, puede corregir los problemas y, a continuación, invocar manualmente la API `registerVM` para volver a registrar la máquina virtual.

Realizar una copia de seguridad de una máquina virtual de servicio de máquina virtual

En vSphere IaaS Control Plane, puede realizar copias de seguridad automáticas de las máquinas virtuales de servicio de máquina virtual a través de una solución de partner de copia de seguridad, como Veeam, que utiliza VMware vSphere Storage APIs – Data Protection.

Por lo general, el administrador de vSphere utiliza la solución del partner para realizar las siguientes tareas:

- Configurar la infraestructura de copia de seguridad, incluida la instalación del software de copia de seguridad y la configuración de los repositorios y el almacenamiento de copias de seguridad.
- Crear un trabajo de copia de seguridad para una máquina virtual o un grupo de máquinas virtuales.
- Iniciar las copias de seguridad activando el trabajo.

Cuando se activa, el software del partner realiza una copia de seguridad de la configuración, los datos y el estado de Kubernetes de la máquina virtual.

Por lo general, la copia de seguridad incluye los siguientes elementos:

- Configuración de la máquina virtual almacenada en vCenter Server.
- Archivo VMX.
- Contenido de los discos de datos de máquina virtual que pueden ser estáticos o FCD.

Para las máquinas virtuales de servicio de máquina virtual, la copia de seguridad también incluye el estado de Kubernetes de la máquina virtual y los recursos adicionales necesarios para arrancar la máquina virtual tras una restauración.

Para obtener más información sobre VMware vSphere Storage APIs – Data Protection y cómo utilizar las soluciones de copia de seguridad de los partners, consulte el artículo 1021175 de la base de conocimientos y la documentación de su partner.

Restaurar una máquina virtual de servicio de máquina virtual

Cuando sea necesario, el administrador de vSphere puede utilizar la copia de seguridad para restaurar la máquina virtual. Por ejemplo, puede restaurar una máquina virtual en la que se produzca un error.

vSphere IaaS Control Plane solo admite la restauración completa de las máquinas virtuales, que restaura una máquina virtual completa a partir de un archivo de copia de seguridad al estado más reciente de la máquina virtual original.

Para realizar este tipo de restauración, asegúrese de que la máquina virtual original no exista en el Supervisor y vSphere. Si aún existe, utilice el comando `kubectl delete vm` en el Supervisor antes de activar el trabajo de restauración.

Después de activar el proceso de restauración desde el software de copia de seguridad, el software de copia de seguridad vuelve a crear la máquina virtual en el grupo de recursos y la carpeta especificados durante la restauración. La máquina virtual se puede restaurar con el mismo nombre de máquina virtual o con uno diferente.

Si el proceso se realiza correctamente, vSphere IaaS Control Plane detecta y registra automáticamente la máquina virtual restaurada en el Supervisor en el mismo espacio de nombres de vSphere donde se creó originalmente. Durante el proceso de restauración, se crea un recurso de máquina virtual en el Supervisor. Si corresponde, también se crean recursos adicionales, como un secreto para arrancar la máquina virtual o PersistentVolumeClaims para los volúmenes adicionales utilizados por la máquina virtual.

Para obtener más información sobre los secretos, consulte la documentación de Kubernetes en https://kubernetes.io/docs/concepts/configuration/secret/. Para obtener información sobre los volúmenes persistentes, consulte https://kubernetes.io/docs/concepts/storage/persistent-volumes/.

Directrices y consideraciones

Al restaurar la máquina virtual, tenga en cuenta lo siguiente:

- Antes de iniciar el proceso de restauración, asegúrese de realizar los siguientes pasos:
  - Compruebe que la máquina virtual original se haya eliminado del Supervisor y vSphere. Si aún existe, utilice el comando `kubectl delete vm` en el Supervisor para eliminarla.

  - Compruebe que la infraestructura subyacente no haya cambiado entre la copia de seguridad y la restauración. Asegúrese de que todos los recursos adecuados que usó la máquina virtual original, como las clases de máquina virtual y las directivas de almacenamiento, estén intactos en el espacio de nombres de vSphere de destino.

    De lo contrario, se produce un error en el registro automático de la máquina virtual.

- La máquina virtual restaurada se registra en el mismo espacio de nombres de vSphere de destino donde se creó originalmente.
- El nombre de la carpeta y el grupo de recursos de destino deben ser los mismos que los que tenía la máquina virtual original.
- El nombre de la máquina virtual restaurada puede ser el mismo que el nombre de la máquina virtual original. También puede utilizar un nombre de máquina virtual diferente.

Lea los siguientes temas a continuación:

- Registrar manualmente una máquina virtual de servicio de máquina virtual

Registrar manualmente una máquina virtual de servicio de máquina virtual

Si, por algún motivo, el registro automático de la máquina virtual no se realiza correctamente, recibirá un mensaje de error que le notifica sobre los problemas exactos que provocan el error. Después de corregir los problemas, puede invocar la API `registerVM` y utilizar el moID de la máquina virtual para registrar manualmente la máquina virtual.

El siguiente ejemplo utiliza los comandos de la CLI del centro de datos (DCLI) para registrar la máquina virtual.

Procedimiento

1. Obtenga el moID de la máquina virtual que se va a registrar.

   ```
   # dcli com vmware vcenter vm list
   ```

   El moID, también denominado ID de MORef, se compone del prefijo vm, seguido de un identificador numérico; por ejemplo, vm-123456.

2. Registre manualmente la máquina virtual.

   ```
   # dcli com vmware vcenter namespaces instances registervm --namespace my-namespace --vm
   vm-123456 +username my-username +password my-password
   ```

   El comando devuelve un tarea similar a la siguiente:

   ```
   task-637:6b051692-7aff-4d59-8a3f-699d114d37e3
   ```

3 Utilice el servicio de tareas de VAPI para obtener el estado de la tarea.

```
# dcli com vmware cis tasks get --task task-637:6b051692-7aff-4d59-8a3f-699d114d37e3
+username my-username +password my-password
```

El comando devuelve el estado de la tarea y cualquier mensaje de error si no es correcto.

Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere

6

Puede utilizar el complemento complemento de Velero para vSphere para crear copias de seguridad y restaurar cargas de trabajo que se ejecutan en pods de vSphere.

Descripción general

Puede utilizar el complemento complemento de Velero para vSphere para realizar copias de seguridad y restaurar cargas de trabajo que se ejecutan en pods de vSphere de Supervisor. Puede realizar copias de seguridad y restaurar aplicaciones sin estado y con estado que se ejecutan en pods de vSphere. Para las aplicaciones con estado, utilice el complemento complemento de Velero para vSphere para crear instantáneas de los volúmenes persistentes (Persistent Volumes, VA).

Nota No puede usar Velero independiente con Restic para realizar copias de seguridad y restaurar pods de vSphere. Debe utilizar el complemento complemento de Velero para vSphere instalado en Supervisor.

Requisitos previos

Antes de poder realizar una copia de seguridad y restaurar pods de vSphere, debe instalar y configurar el complemento de complemento de Velero para vSphere. Consulte #unique_20.

Nota El complemento de complemento de Velero para vSphere no realiza una copia de seguridad ni restaura el estado de Supervisor.

Realizar una copia de seguridad de pod de vSphere

Para realizar una copia de seguridad de pod de vSphere sin estado, ejecute el siguiente comando:

```
velero backup create <backup name> --include-namespaces=my-namespace
```

La copia de seguridad se marca como `Completed` después de que se hayan tomado todas las instantáneas locales y de que los metadatos de Kubernetes se carguen en el almacén de objetos. Sin embargo, la copia de seguridad de las instantáneas de volumen se produce de forma asíncrona y puede seguir ocurriendo en segundo plano y tardar algún tiempo en completarse.

Puede comprobar el estado de las instantáneas de volumen supervisando instantáneas y cargando recursos personalizados.

CRD de instantánea

Para cada instantánea de volumen, se crea un recurso personalizado de instantánea en el mismo espacio de nombres que la PVC a la que se crea la instantánea. Puede obtener todas las instantáneas en el espacio de nombres de PVC ejecutando el siguiente comando.

```
kubectl get -n <pvc namespace> snapshot
```

La CRD de instantánea tiene varias fases para el campo de `status.phase`, entre ellas, las siguientes:

Estado	Descripción
Novedad	Aún no procesada
Snapshotted	Se tomó una instantánea local
SnapshotFailed	Se produjo un error en la instantánea local
Uploading	Se está cargando la instantánea
Uploaded	Se cargó la instantánea
UploadFailed	No se pudo cargar la instantánea
Canceling	Se está cancelando la carga de la instantánea
Canceled	Se canceló la carga de la instantánea
CleanupAfterUploadFailed	Error en la limpieza de la instantánea local después de la carga de la instantánea

Cargar CRD

Para cada instantánea de volumen que se cargará en el almacén de objetos, se creará un CR de carga en el mismo espacio de nombres que Velero. Puede obtener todas las cargas en el espacio de nombres de Velero ejecutando el siguiente comando.

```
kubectl get -n <velero namespace> upload
```

La carga de CRD tiene varias fases para el campo de `status.phase`, entre las que se incluyen las siguientes:

Estado	Descripción
Novedad	Aún no procesada
InProgress	Carga en curso
UploadError	Error al cargar

Estado	Descripción
CleanupFailed	Error al eliminar la instantánea local después de la carga Se reintentará
Canceling	Se está cancelando la carga Puede producirse si se llama a `velero backup delete` mientras la carga de instantáneas está en curso
Canceled	Carga cancelada

Las cargas de errores de carga se volverán a intentar periódicamente. En ese momento, su fase volverá a En curso. Una vez que una carga se haya completado correctamente, su registro permanecerá durante un período de tiempo y, finalmente, se eliminará.

Restaurar una pod de vSphere

Para restaurar una carga de trabajo de pod de vSphere de la que se realizó una copia de seguridad mediante el complemento complemento de Velero para vSphere, realice los siguientes pasos.

1 Cree un espacio de nombres de vSphere para la carga de trabajo que restaurará.

2 Configure la directiva de almacenamiento para el espacio de nombres.

3 Ejecute el siguiente comando de Velero para restaurar la carga de trabajo:

```
velero restore create --from-backup backup-name
```

La restauración de Velero se marcará como `Completed` cuando las instantáneas de volumen y otros metadatos de Kubernetes se hayan restaurado correctamente en el clúster actual. En este punto, también se completan todas las tareas del complemento de vSphere relacionadas con esta restauración. En el caso de las copias de seguridad de Velero, no hay tareas de movimiento de datos asíncronas por detrás.

Antes de que la restauración de Velero sea `Completed`, puede comprobar el estado de la restauración de volúmenes supervisando CloneFromSnapshots/Descargar CSR como se indica a continuación.

CRD de CloneFromSnapshots

Para la restauración a partir de cada instantánea de volumen, se creará un CR de CloneFromSnapshots en el mismo espacio de nombres que la PVC a la que se creó originalmente una instantánea. Podemos obtener todos los CloneFromSnapshots de PVC ejecutando el siguiente comando.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

CRD de CloneFromSnapshots tiene varias fases para el campo `status.phase`, entre ellas las siguientes:

Estado	Descripción
Novedad	No se completó la clonación de la instantánea
Completed	Se completó la clonación de la instantánea
Con errores	Error en la clonación de instantánea

Descargar CRD

Desde cada restauración de instantánea de volumen que se descargará del almacén de objetos, se creará un CR de descarga en el mismo espacio de nombres que Velero. Podemos obtener todas las descargas en el espacio de nombres de Velero ejecutando el siguiente comando.

```
kubectl -n <velero namespace> get download
```

La CRD de descarga tiene varias fases para el campo `status.phase`, entre las que se incluyen las siguientes:

Estado	Descripción
Novedad	Aún no procesada
InProgress	Descarga en curso
Completed	Se completó la descarga
Retry	Se volverá a intentar la descarga. Cuando se produce un error durante la descarga de los datos de copia de seguridad, se vuelve a intentar la descarga
Con errores	Error en la descarga

Solucionar problemas de copia de seguridad y restauración de vSphere IaaS Control Plane

7

Aprenda a solucionar problemas relacionados con la copia de seguridad y restauración de vSphere IaaS Control Plane.

Lea los siguientes temas a continuación:

Limpiar objetos huérfanos después de una restauración de Supervisor a partir de una copia de seguridad

Después de restaurar Supervisor a partir de una copia de seguridad, todos los recursos de K8s que se creen después de que se realice la copia de seguridad se eliminarán cuando se complete la restauración. Si algunos de estos recursos se asociaron con objetos, como máquinas virtuales o discos, quedarán huérfanos en vCenter Server. Debe limpiar los objetos huérfanos de vCenter Server.

Procedimiento

1 Enumere todas las máquinas virtuales de un espacio de nombres de vSphere.

a Recupere `folderMoId` para el espacio de nombres de vSphere ejecutando el siguiente comando en una máquina virtual de plano de control de Supervisor:

```
root@421c9fa40208448fecc15d277bdca66d [ ~ ]# kubectl get availabilityzone -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "topology.tanzu.vmware.com/v1alpha1",
            "kind": "AvailabilityZone",
            "metadata": {
                ...
            },
            "spec": {
                "clusterComputeResourceMoIDs": [
                    "domain-c50"
                ],
                "clusterComputeResourceMoId": "domain-c50",
                "namespaces": {
                    "pod-ns": {
                        "folderMoId": "group-v81", <--- this is the folderMoId that
you need for next step
                        ...
                    },
                    "vmsvc-ns": {
                        "folderMoId": "group-v83", <--- this is the folderMoId that
you need for next step
                        ...
                    }
                }
            }
        }
    ],
    "kind": "List",
    "metadata": {
        "resourceVersion": ""
    }
}
```

b Enumere todas las máquinas virtuales existentes en el espacio de nombres de vSphere ejecutando el siguiente comando DCLI:

En el ejemplo, se usa el espacio de nombres `pod-ns`

```
root@sc2-10-186-199-30 [ ~ ]# dcli +i +username ‘Administrator@vsphere.local’
+password <password>
Welcome to VMware Datacenter CLI (DCLI)

usage: <namespaces> <command>
```

```
To auto-complete and browse DCLI namespaces:   [TAB]
If you need more help for a command:           vcenter vm get --help
If you need more help for a namespace:         vcenter vm --help
To execute dcli internal command: env
For detailed information on DCLI usage visit:  http://vmware.com/go/dcli

dcli> com vmware vcenter vm list --folders group-v81
|---------------|-----|----------------------------------------|-----------|---------|
|memory_size_MiB|vm   |name                                    |power_state|cpu_count|
|---------------|-----|----------------------------------------|-----------|---------|
|512            |vm-84|deployment-before-backup-778449d88d-c9gnc|POWERED_ON |1        |
|512            |vm-85|deployment-before-backup-778449d88d-4jtqj|POWERED_ON |1        |
|512            |vm-86|deployment-before-backup-778449d88d-tqwbh|POWERED_ON |1        |
|512            |vm-91|deployment-after-backup-778449d88d-khkxx |POWERED_OFF|1        |
|512            |vm-92|deployment-after-backup-778449d88d-7dgcc |POWERED_OFF|1        |
|512            |vm-93|deployment-after-backup-778449d88d-sxbcf |POWERED_OFF|1        |
|---------------|-----|----------------------------------------|-----------|---------|
```

.

2 Busque espacios de nombres huérfanos y límpielos.

Si se elimina un espacio de nombres después de realizar una copia de seguridad de Supervisor, ese espacio de nombres se volverá a crear después de la restauración de Supervisor como un recurso de Kubernetes. Debe eliminar ese recurso de K8s.

a Para buscar el espacio de nombres huérfano, enumere todos los espacios de nombres en vCenter Server.

```
dcli> com vmware vcenter namespaces instances list
```

b Enumere todos los recursos de K8s del espacio de nombres.

```
root@423f9d75bef000dc828a535c6ac0bd4b [ ~ ]# k get ns -A
```

a Busque las diferencias entre los objetos resultantes de los pasos A y B, y limpie los recursos huérfanos de K8s del espacio de nombres.

```
root@423f9d75bef000dc828a535c6ac0bd4b [ ~ ]# k delete ns test-set-workload-ns
namespace "test-set-workload-ns" deleted
```

3 Busque las máquinas virtuales huérfanas asociadas con los recursos de `VirtualMachine` y límpielas.

Los recursos de Kubernetes de `VirtualMachine` que se creen después de realizar la copia de seguridad de Supervisor generarán máquinas virtuales huérfanas una vez que se restaure Supervisor a partir de esa copia de seguridad. Debe limpiar estas máquinas virtuales huérfanas del inventario de vCenter Server.

a Busque máquinas virtuales huérfanas asociadas con recursos de `VirtualMachine`.

Los pasos que se indican a continuación utilizan el espacio de nombres `vmsvc-ns` como ejemplo.

1 Enumere todas las máquinas virtuales del inventario de vCenter Server. En el ejemplo, se enumeran todas las máquinas virtuales de vCenter Server, ya que `group-96` está asociado con el espacio de nombres `vmsvc-ns`.

```
dcli> com vmware vcenter vm list --folders group-v96
|---------------|------|------------|-----------|---------|
|memory_size_MiB|vm    |name        |power_state|cpu_count|
|---------------|------|------------|-----------|---------|
|2048           |vm-104|vmsvc-after |POWERED_ON |2        |
|2048           |vm-97 |vmsvc-before|POWERED_ON |2        |
|---------------|------|------------|-----------|---------|
```

2 Enumere todos los recursos de K8s de `VirtualMachine`. Ejecute `kubectl get` para obtener los detalles de los recursos en cualquiera de las máquinas virtuales del plano de control y busque `uniqueID` en los resultados. En el ejemplo, la lista de máquinas virtuales asociada a los recursos de K8s es `vm-97`.

```
root@42344b596f57bfcf9441179fa1ed1a5c [ ~ ]# k get vm -n vmsvc-ns -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "vmoperator.vmware.com/v1alpha1",
            "kind": "VirtualMachine",
            ...
            "uniqueID": "vm-97",
...
}
```

3 Busque las diferencias entre las dos listas resultantes de los pasos anteriores.

- La lista de máquinas virtuales en vCenter Server: `<vm-104, vm-97>`
- La lista de máquinas virtuales asociada a los recursos de k8s: `<vm-97>`

Por lo tanto, la lista de máquinas virtuales huérfanas es: `<vm-104>`.

b Limpie las máquinas virtuales huérfanas.

```
dcli> com vmware vcenter vm power stop --vm vm-104
dcli> com vmware vcenter vm delete --vm vm-104
```

4 Busque las máquinas virtuales huérfanas asociadas con recursos del pod y límpielas.

Los recursos de K8s del pod que se creen después de realizar la copia de seguridad de Supervisor generarán máquinas virtuales huérfanas en vCenter Server después de la restauración de Supervisor. Siga los pasos para encontrarlos y limpiarlos.

En los ejemplos se utiliza el espacio de nombres pod-ns.

a Enumere todas las máquinas virtuales del inventario de vCenter Server.

En el ejemplo, el grupo de máquinas virtuales group-v83 está asociado con el espacio de nombres pod-ns. La lista de máquinas virtuales es vm-88, vm-89, vm-90, vm-101, vm-102 y vm-103.

```
dcli> com vmware vcenter vm list --folders group-v83
|---------------|------|-----------------------------------------|-----------|---------
|
|memory_size_MiB|vm    |name                                     |power_state|
cpu_count|
|---------------|------|-----------------------------------------|-----------|---------
|
|512            |vm-101|deployment-after-backup-778449d88d-ldvn8 |POWERED_OFF|1
|
|512            |vm-102|deployment-after-backup-778449d88d-v29dd |POWERED_OFF|1
|
|512            |vm-103|deployment-after-backup-778449d88d-zdbl9 |POWERED_OFF|1
|
|512            |vm-88 |deployment-before-backup-778449d88d-fgq5b|POWERED_ON |1
|
|512            |vm-89 |deployment-before-backup-778449d88d-mp7td|POWERED_ON |1
|
|512            |vm-90 |deployment-before-backup-778449d88d-cjhq6|POWERED_ON |1
|
|---------------|------|-----------------------------------------|-----------|---------
|
```

b Enumere los recursos de K8s.

Ejecute kubectl get para obtener detalles de recursos en cualquiera de las máquinas virtuales del plano de control y busque vmware-system-vm-moid en los resultados. La lista de máquinas virtuales asociada a los recursos de K8s es vm-88, vm-89 y vm-90.

```
root@42344b596f57bfcf9441179fa1ed1a5c [ ~ ]# k get pod -n pod-ns -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "v1",
            "kind": "Pod",
            "metadata": {
                "annotations": {
                    ...
                    "vmware-system-vm-moid": "vm-90:5a5198fc-c5cb-4b89-
a70f-331025b40539",
                    ...
                },
                    ...
                    "vmware-system-vm-moid": "vm-88:5a5198fc-c5cb-4b89-
a70f-331025b40539",
```

```
                    ...
                    "vmware-system-vm-moid": "vm-89:5a5198fc-c5cb-4b89-
a70f-331025b40539",
                    ...
}
```

c Busque las diferencias entre las dos listas resultantes de los pasos anteriores.

- La lista de máquinas virtuales en vCenter Server es: `<vm-88, vm-89, vm-90, vm-101, vm-102, vm-103>`
- La lista de máquinas virtuales asociada a los recursos de K8s es: `<vm-88, vm-89, vm-90>`

Por lo tanto, la lista de máquinas virtuales huérfanas es: `<vm-101, vm-102, vm-103>`

d Limpie las máquinas virtuales huérfanas.

```
dcli> com vmware vcenter vm delete --vm vm-101
dcli> com vmware vcenter vm delete --vm vm-102
dcli> com vmware vcenter vm delete --vm vm-103
```

5 Busque las máquinas virtuales y los grupos de recursos huérfanos asociados con clústeres de Tanzu Kubernetes Grid y límpielos.

Los clústeres de Tanzu Kubernetes Grid que se creen después de realizar la copia de seguridad de Supervisor también generarán máquinas virtuales huérfanas en vCenter Server después de la restauración de Supervisor.

Nota Si tuvo algún problema al crear clústeres de TKG después de la operación de restauración, debe limpiar las máquinas virtuales huérfanas según las instrucciones del paso actual.

a Busque la lista de clústeres de Tanzu Kubernetes Grid huérfanos.

Utilice kubectl para obtener la lista de recursos de K8s del clúster de Tanzu Kubernetes Grid en cualquiera de las máquinas virtuales del plano de control: `<test-cluster, test-cluster-e2e-script, tkc-before-backup>`.

```
root@4239f4159c7063d5608cf3fc0bdd532e [ ~ ]# k get tkc -A
NAMESPACE             NAME                      CONTROL PLANE   WORKER   TKR
NAME                   AGE   READY   TKR COMPATIBLE   UPDATES AVAILABLE
selfservice-tkc-ns    test-cluster              1               1        v1.23.8---
vmware.3-tkg.1   19h   True    True
test-gc-e2e-demo-ns   test-cluster-e2e-script   3               1        v1.23.8---
vmware.3-tkg.1   18h   False   True
tkc-ns                tkc-before-backup         3               1        v1.23.8---
vmware.3-tkg.1   16h   True    True
```

Use DCLI para obtener todos los grupos de recursos asociados con el espacio de nombres o el clúster de Tanzu Kubernetes Grid y, a continuación, obtenga la lista de clústeres de Tanzu Kubernetes Grid en vCenter Server: `<test-cluster, test-cluster-e2e-script, tkc-before-backup, tkc-after-backup>`

```

dcli> com vmware vcenter resourcepool list
|-----------------------|-------------|
|name                   |resource_pool|
|-----------------------|-------------|
|Resources              |resgroup-10  |
|Resources              |resgroup-23  |
|Namespaces             |resgroup-56  |
|selfservice-tkc-ns     |resgroup-62  | <--- this is a namespace
|test-cluster           |resgroup-66  | <--- Tanzu Kubernetes Grid cluster
|test-gc-e2e-demo-ns    |resgroup-70  | <--- this is a namespace
|test-cluster-e2e-script|resgroup-74  | <--- Tanzu Kubernetes Grid cluster
|tkc-ns                 |resgroup-80  | <--- this is a namespace
|tkc-before-backup      |resgroup-89  | <--- Tanzu Kubernetes Grid cluster
|tkc-after-backup       |resgroup-96  | <--- Tanzu Kubernetes Grid cluster
|-----------------------|-------------|
```

b Si se comparan las dos listas de los pasos anteriores, la lista de clústeres de Tanzu Kubernetes Grid huérfanos es: `<tkc-after-backup>`

c Limpie las máquinas virtuales asociadas con el clúster de Tanzu Kubernetes Grid huérfano.

Utilice DCLI para obtener todas las máquinas virtuales asociadas con el clúster de Tanzu Kubernetes Grid huérfano mediante el grupo de recursos asociado `<resgroup-96>`:

```
dcli> com vmware vcenter vm list --resource-pools resgroup-96
|---------------|------|----------------------------------------------|-----------|---
------|
|memory_size_MiB|vm    |name                                          |power_state|
cpu_count|
|---------------|------|----------------------------------------------|-----------|---
------|
|2048           |vm-100|tkc-after-backup-zlcdm-wk5xf                  |POWERED_ON |
2        |
|2048           |vm-101|tkc-after-backup-zlcdm-76q4h                  |POWERED_ON |
2        |
|2048           |vm-98 |tkc-after-backup-zlcdm-9fv2w                  |POWERED_ON |
2        |
|2048           |vm-99 |tkc-after-backup-workers-4hdqb-657fb58d45-d7pqg|POWERED_ON |
2        |
|---------------|------|----------------------------------------------|-----------|---
------|
```

A continuación, elimine las máquinas virtuales una por una:

```
dcli> com vmware vcenter vm power stop --vm vm-100
dcli> com vmware vcenter vm delete --vm vm-100
```

d Limpie el grupo de recursos asociado con el clúster de Tanzu Kubernetes Grid huérfano.

```
<dcli> com vmware vcenter resourcepool delete --resource-pool resgroup-96
```

También puede eliminar el grupo de recursos huérfano de vSphere Client.

6 Busque los FCD (discos de primera clase) huérfanos asociados con los volúmenes permanentes (PV) y límpielos.

Los recursos de K8s de PV creados después de realizar la copia de seguridad de Supervisor generarán FCD huérfanos en vCenter Server después de la restauración de Supervisor. Siga los pasos para encontrarlos y limpiarlos.

a Busque los FCD huérfanos asociados con los PV.

1 Instale govc, que utilizará para encontrar los FCD huérfanos. Govc es una alternativa de la CLI a la interfaz de usuario fácil de usar y adecuada para tareas de automatización.

```
curl -L -o - "https://github.com/vmware/govmomi/releases/latest/download/govc_$
(uname -s)_$(uname -m).tar.gz" | tar -C /usr/local/bin -xvzf - govc
```

Hay más opciones de instalación disponibles en https://github.com/vmware/govmomi/tree/main/govc#installation.

2 Ejecute el siguiente script de Bash para enumerar los PV que existen en Supervisor.

```

#!/bin/bash

export GOVC_INSECURE=1
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk

# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc volume.ls -l -ds=<datastore path>
```

Y el resultado:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
590c8e31-f5bf-4179-9250-5cdd66bf591c
pvc-843c932b-8974-475d-8f8a-9b165137169d    1.0GB   KUBERNETES
vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-b80eb76becdf
37f8ad5b-dfe6-465b-b0f0-11591a2968dc    pvc-77c42590-
f0b0-457f-9743-6a3ebca55078    1.0GB   KUBERNETES
vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-b80eb76becdf
28a265b8-2e6b-421c-b16d-046ffc7aeea7    pvc-1b88c923-4354-4537-a7cb-
a8a6d763d5e7    1.0GB   KUBERNETES  vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-
b80eb76becdf
```

3 Ejecute el siguiente script de Bash para enumerar todos los discos en vCenter Server:

```
#!/bin/bash

export GOVC_INSECURE=1
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk
```

```
# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc disk.ls -l -ds=<datastore path>
```

Y el resultado:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
28a265b8-2e6b-421c-b16d-046ffc7aeea7  pvc-1b88c923-4354-4537-a7cb-a8a6d763d5e7
1.0G    Jul  4 02:33:27 <--- this is the disk correspondings to PV
37f8ad5b-dfe6-465b-b0f0-11591a2968dc  pvc-77c42590-f0b0-457f-9743-6a3ebca55078
1.0G    Jul  4 02:32:41 <--- this is the disk correspondings to PV
3a7517c2-f8c2-46a9-b0d5-18c665759311  vmware-sv-img-cache-domain-c50
26.0M   Jul  4 02:36:41
590c8e31-f5bf-4179-9250-5cdd66bf591c  pvc-843c932b-8974-475d-8f8a-9b165137169d
1.0G    Jul  4 02:30:45 <--- this is the disk correspondings to PV
68ba220c-0f83-49eb-b77a-d60471e24844  pvc-92f83ae0-7c2d-46d9-ab85-19858462ddd1
5.0G    Jul  4 18:27:02 <--- this is the disk correspondings to PV
72dbe8c5-a3b5-4298-8203-ea1cb86116e6  vmware-sv-img-cache-domain-c50
3.0M    Jul  4 02:38:39
79e233a6-0134-40e7-8ba8-3133442324f9  vmware-sv-img-cache-domain-c50
195.0M  Jul  4 18:26:12
a1a0a9d7-0baf-4592-9041-8c0feb960246  vmware-sv-img-cache-domain-c50
7.0M    Jul  4 02:35:37
cec2af09-80af-4086-a069-34140e2480dc  vmware-sv-img-cache-domain-c50
193.0M  Jul  4 02:31:12
```

4 Compare las dos listas de los pasos anteriores.

- La lista de PV: `<590c8e31-f5bf-4179-9250-5cdd66bf591c, 37f8ad5b-dfe6-465b-b0f0-11591a2968dc, 28a265b8-2e6b-421c-b16d-046ffc7aeea7>`
- La lista de FCD: `<590c8e31-f5bf-4179-9250-5cdd66bf591c, 37f8ad5b-dfe6-465b-b0f0-11591a2968dc, 28a265b8-2e6b-421c-b16d-046ffc7aeea7, 68ba220c-0f83-49eb-b77a-d60471e24844>`

Los FCD huérfanos son: `<68ba220c-0f83-49eb-b77a-d60471e24844>`

b Elimine los FCD huérfanos.

Utilice govc para eliminar los FCD huérfanos; script de ejemplo:

```
#!/bin/bash

export GOVC_INSECURE=1
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk

# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc disk.rm -ds=<datastore path> 68ba220c-0f83-49eb-b77a-d60471e24844
```

Y el resultado:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
[06-07-23 11:36:27] Deleting 68ba220c-0f83-49eb-b77a-d60471e24844...OK
```